Prosti brojevi

Pružinac, Patricia

Master's thesis / Diplomski rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, School of Applied Mathematics and Informatics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet primijenjene matematike i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:334279

Sveučilište Josipa Jurja Strossmayera u Osijeku

Fakultet primijenjene matematike i informatike

Sveučilišni integrirani nastavnički studij matematike i informatike

Prosti brojevi

Diplomski rad

Mentor:

izv. prof. dr. sc. Mirela Jukić Bokun

Student:

Patricia Pružinac

Osijek, 2024

Sadržaj

Uvod

Prosti brojevi jedan su od najvećih misterija koji zaokupljaju umove matematičara više od 2 tisućljeća. Počevši od Euklidovog dokaza o postojanju beskonačno mnogo prostih brojeva sve do nedavnog otkrića prostoga broja s 22 862 048 znamenki, uloženi su brojni napori kako bi se otkrile tajne koje kriju ovi naizgled jednostavni brojevi. Oni se smatraju gradivnim blokovima svih prirodnih brojeva većih od 1, a njihova primjena na problemima iz svakodnevnoga života, posebno u kriptografiji i računalnoj znanosti, vrijedna je pažnje.

Ovaj rad sastoji se od 5 poglavlja:

1: U ovome poglavlju dat ćemo kratak osvrt na osnovne pojmove i rezultate vezane uz djeljivost i kongruencije.

2: Uvest ćemo pojam prostih brojeva i navesti njihova osnovna svojstva (osnovni teorem aritmetike, Euklidov dokaz o postojanju beskonačno mnogo prostih brojeva, Eratostenovo sito). Potom ćemo definirati proste brojeve posebnoga oblika (Fermatovi, Mersenneovi, Sophieini) i na samome kraju opisati važna otkrića vezana uz distribuciju prostih brojeva.

3: U ovome ćemo se poglavlju baviti testovima prostosti. Prva dva dijela obuhvatit će deterministčke (probno dijeljenje, AKS, Lucas – Lehmer, Pepin) i vjerojatnosne (Fermat, Miller – Rabin, Solovay – Strassen) testove te prikladne algoritme za svaki, dok ćemo u trećem dijelu definirati eliptičke krivulje i dati korake za dokazivanje prostosti pomoću njih.

4: U predzadnjem ćemo poglavlju opisati najpoznatiju primjenu prostih brojeva u kriptografiji, tj. u RSA kriptosustavu čija se sigurnost temelji na teškome problemu pronalazaka prostih faktora. Na kraju ćemo spomenuti potencijalnu modernu alternativu temeljenu na kriptosustavima u čijem su središtu eliptičke krivulje i koja nudi jednaku sigurnost uz korištenje manje memorije.

5: Zadnje ćemo poglavlje posvetiti nedokazanim slutnjama u teoriji brojeva koje su vezane uz proste brojeve (de Polignac, Lagrange, Goldbach, Landau).

1 | Djeljivost i kongruencije

U ovome poglavlju prisjetit ćemo se definicija i teorema vezanih uz pojmove djeljivosti i kongruencija koje su potrebne za daljnje razumijevanje rada.

1.1 Djeljivost

Definicija 1. *Neka su $a \in \mathbb{Z} \setminus \{0\}$ i $b \in \mathbb{Z}$. Kažemo da a dijeli b, i pišemo $a|b$, ako postoji $d \in \mathbb{Z}$ takav da vrijedi $b = ad$. U slučaju da takav d ne postoji, kažemo da a ne dijeli b i pišemo $a \nmid b$.*

Broj a iz Definicije 1 nazivamo djeliteljem broja b, a broj b višekratnikom broja a. Direktne posljedice Definicije 1 dane su u sljedećem teoremu:

Teorem 1 (Svojstva djeljivosti, vidi [6])**.** *Neka su $a, b, c \in \mathbb{Z}$. Vrijedi sljedeće:*

i) $1|a$.

ii) $a|0$ *i* $a|a$, *za sve* $a \in \mathbb{Z} \setminus \{0\}$.

iii) $a|1$ *ako i samo ako je* $a \in \{1, -1\}$.

iv) *Ako* $a|b$ *i* $c|d$, *onda* $ac|bd$.

v) *Ako* $a|b$ *i* $b|c$, *onda* $a|c$.

vi) $a|b$ *i* $b|a$ *ako i samo ako je* $a \in \{b, -b\}$.

vii) *Ako* $a|b$ *i* $b \neq 0$, *onda* $|a| \leq |b|$.

viii) *Ako* $a|b$ *i* $a|c$, *onda* $a|(bx + cy)$, *za proizvoljne* $x, y \in \mathbb{Z}$.

Definicija 2. *Neka su $a, b \in \mathbb{Z}$ takvi da je $a^2 + b^2 \neq 0$. Najveći zajednički djelitelj brojeva a i b, u oznaci (a, b), broj je $d \in \mathbb{N}$ koji zadovoljava sljedeća dva svojstva:*

i) $d|a$ *i* $d|b$.

ii) *Ako* $c|a$ *i* $c|b$, *onda je* $c \leq d$.

Teorem 2 (Teorem o dijeljenju s ostatkom, vidi [17])**.** *Neka su $a \in \mathbb{Z}$ i $b \in \mathbb{N}$. Tada postoje jedinstveni $q, r \in \mathbb{Z}$ takvi da je*

$$a = qb + r,$$

pri čemu je $0 \leq r < b$.

Broj r iz prethodnoga teorema naziva se ostatak, a broj q kvocijent cjelobrojnog dijeljenja broja a brojem b.
Uzastopnom primjenom Teorema 2 dobivamo Euklidov algoritam pomoću kojega možemo odrediti najveći zajednički djelitelj dvaju brojeva. On je dan sljedećim nizom jednakosti:

$$\begin{aligned} a &= q_1 b + r_1, & 0 \leq\ & r_1 < b, \\ b &= q_2 r_1 + r_2, & 0 \leq\ & r_2 < r_1, \\ r_1 &= q_3 r_2 + r_3, & 0 \leq\ & r_3 < r_2, \\ &\vdots & & \\ r_{n-2} &= q_n r_{n-1} + r_n, & 0 \leq\ & r_n < r_{n-1}, \\ r_{n-1} &= q_{n+1} r_n + 0. & & \end{aligned}$$

Vrijedi $(a, b) = r_n$ (vidi [6]).

Teorem 3 (vidi [6]). *Za dane brojeve $a, b \in \mathbb{Z}$ takve da je $a^2 + b^2 \neq 0$, postoje $x, y \in \mathbb{Z}$ takvi da je*

$$ax + by = (a, b). \tag{1.1}$$

Jednakost (1.1) naziva se Bezoutov identitet.
Rješivost jednadžbi takvoga oblika dana je u sljedećem teoremu:

Teorem 4 (vidi [14]). *Neka su $a, b \in \mathbb{Z}$. Najmanji broj $m \in \mathbb{N}$ za koji postoji cjelobrojno rješenje jednadžbe $ax + by = m$[1] je (a, b). Štoviše, jednadžba $ax + by = m$ ima cjelobrojno rješenje ako i samo ako $(a, b) | m$.*

Definicija 3. *Neka su $a, b \in \mathbb{Z}$ takvi da je $a^2 + b^2 \neq 0$. Kažemo da su a i b relativno prosti ako je $(a, b) = 1$.*

Karakterizacija relativno prostih brojeva u terminima linearnih kombinacija dana je sljedećim teoremom:

Teorem 5 (vidi [6]). *Neka su $a, b \in \mathbb{Z}$ takvi da je $a^2 + b^2 \neq 0$. Brojevi a i b relativno su prosti ako i samo ako postoje $x, y \in \mathbb{Z}$ takvi da je $ax + by = 1$.*

Lema 1 (Euklidova lema, vidi [6]). *Ako $a | bc$ i $(a, b) = 1$, onda $a | c$.*

Definicija 4. *Pravi djelitelj broja n svaki je pozitivan djelitelj d od n takav da je $1 \leq d < n$.*

Definicija 5. *Neka je $n \in \mathbb{N}$. Sa $\sigma(n)$ označavamo sumu svih pozitivnih djelitelja broja n, tj. $\sigma(n) = \sum_{d_i | n} d_i$, $d_i > 0$.*

Propozicija 1 (vidi [14]). *Funkcija $\sigma : \mathbb{N} \to \mathbb{N}$ je multiplikativna, tj. $\sigma(1) = 1$ te za svaka dva broja $m, n \in \mathbb{N}$ takva da je $(m, n) = 1$ vrijedi:*

$$\sigma(mn) = \sigma(m)\sigma(n).$$

[1] Jednadžbe ovoga oblika nazivaju se linearne diofantske jednadžbe.

1.2 Kongruencije

Definicija 6. *Neka je $n \in \mathbb{N}$ i neka su $a, b \in \mathbb{Z}$. Kažemo da je a kongruentan b modulo n, u oznaci $a \equiv b \pmod{n}$, ako $n|a-b$.*

Primijetimo da ako je r ostatak pri dijeljenju broja a brojem n, onda je $a \equiv r \pmod{n}$ te vrijedi da $n|a$ ako i samo ako je $a \equiv 0 \pmod{n}$ (vidi [17]).

Svojstva kongruencija dana su sljedećim propozicijama i korolarima:

Propozicija 2 (vidi [17]). *Biti kongruentan modulo n relacija je ekvivalencije na skupu $\mathbb{Z}$, tj. vrijede sljedeća svojstva:*

i) ***refleksivnost:*** $a \equiv a \pmod{n}$;

ii) ***simetričnost:*** $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$;

iii) ***tranzitivnost:*** $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$.

Propozicija 3 (vidi [17]). *Ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$, onda je*

i) $a + c \equiv b + d \pmod{n}$;

ii) $ac \equiv bd \pmod{n}$.

Korolar 1 (vidi [17]). *Ako je $a \equiv b \pmod{n}$, onda za bilo koji $c \in \mathbb{Z}$ vrijedi:*

i) $a + c \equiv b + c \pmod{n}$;

ii) $ac \equiv bc \pmod{n}$.

Propozicija 4 (vidi [17]). *Ako je $ac \equiv bc \pmod{n}$ i $(c, n) = g$, onda je $a \equiv b \pmod{\frac{n}{g}}$.*

Korolar 2 (vidi [17]). *Ako je $ac \equiv bc \pmod{n}$ i $(c, n) = 1$, onda je $a \equiv b \pmod{n}$.*

Propozicija 5 (vidi [17]). *Ako je $a \equiv b \pmod{n}$, onda je $a^k \equiv b^k \pmod{n}$, pri čemu je $k \in \mathbb{N}$.*

Definicija 7. *Neka je $n \in \mathbb{N}, n > 1$. Skup $S = \{a_1, \ldots, a_n\}$ nazivamo potpun sustav ostataka modulo n ako za svaki $b \in \mathbb{Z}$ postoji jedinstveni $a_i \in S$ za koji vrijedi da je $b \equiv a_i \pmod{n}$.*

Definicija 8. *Neka je $n \in \mathbb{N}, n > 1$, i $S = \{a_1, \ldots, a_n\}$ potpun sustav ostataka modulo n. Podskup S' skupa S koji sadrži sve elemente skupa S koji su relativno prosti s n nazivamo reducirani sustav ostataka modulo n.*

Definicija 9. *Neka je $n \in \mathbb{N}$. Broj prirodnih brojeva u nizu $1, 2, \ldots, n$ koji su relativno prosti s n označavamo s $\varphi(n)$. Ovako definiranu funkciju $\varphi : \mathbb{N} \to \mathbb{N}$ nazivamo Eulerova funkcija.*

Uočimo da je $\varphi(n)$ jednak broju elemenata reduciranog sustava ostataka modulo n pa ga možemo označiti i sa $\{a_1, a_2, \ldots, a_{\varphi(n)}\}$.

Teorem 6 (Eulerov teorem, vidi [14]). *Neka je $a \in \mathbb{Z}$ i $n \in \mathbb{N}$. Ako je $(a, n) = 1$, onda je $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

2 | Prosti brojevi

Prosti su brojevi vrlo važan pojam za teoriju brojeva te se smatraju gradivnim blokovima svih prirodnih brojeva većih od 1. Prvu definiciju prostoga broja dao je starogrčki matematičar **Euklid** (oko 330. pr. Kr. – oko 275. pr. Kr.), a ona je glasila ovako: "Prost broj je onaj koji se može mjeriti samo jedinicom". U ovome poglavlju definirat ćemo proste brojeve, iskazati i dokazati važne teoreme vezane uz njih, pogledati proste brojeve posebnoga oblika i, konačno, proučiti distribuciju prostih brojeva.

2.1 Definicija i osnovna svojstva

Definicija 10. *Za prirodan broj p, $p > 1$, kažemo da je prost ako su mu jedini pozitivni djelitelji 1 i p. Za prirodan broj veći od 1 koji nije prost kažemo da je složen.*

Primjer 1. *Pogledajmo prvih deset prirodnih brojeva:* $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$. *Među njima*

- *broj* 1 *nije ni prost ni složen;*
- *brojevi* $2, 3, 5$ *i* 7 *prosti su;*
- *brojevi* $4, 6, 8, 9$ *i* 10 *složeni su.*

Uočavamo da je 2 jedini paran prost broj. Također, možemo zaključiti da će prirodni brojevi veći od 1 biti ili prosti ili složeni. Složene brojeve uvijek ćemo moći zapisati u obliku produkta potencija prostih faktora. Ta je tvrdnja u teoriji brojeva poznata pod nazivom Osnovni teorem aritmetike, a njezine začetke pronalazimo u devetoj knjizi Euklidovih *Elemenata* u obliku Propozicije 14. Prije samoga iskaza i dokaza teorema, navest ćemo i dokazati neke tvrdnje koje će nam za to biti potrebne.

Propozicija 6 (vidi [17])**.** *Neka su $a, b \in \mathbb{Z}$. Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$.*

Dokaz. Nek su $a, b \in \mathbb{Z}$ i p prost broj takav da $p|ab$. Pretpostavimo da p ne dijeli jednog od brojeva a i b, npr. neka $p \nmid a$. Kako je p prost broj, njegovi jedini pozitivni djelitelji su 1 i p, a to implicira da je $(a, p) = 1$ (općenito, $(a, p) = p$ ako $p|a$ i $(a, p) = 1$ ako $p \nmid a$). Prema Lemi 1 $p|b$. □

Prethodna se propozicija može poopćiti na umnožak proizvoljno mnogo faktora:

Korolar 3 (vidi [6]). *Ako je p prost broj takav da $p|a_1a_2\cdots a_n$, onda $p|a_k$ za neki k, pri čemu je $1 \leq k \leq n$.*

Dokaz. Dokaz provodimo matematičkom indukcijom po broju faktora n.
BAZA:
Za $n = 2$ vrijedi da ako $p|a_1a_2$, onda $p|a_1$ ili $p|a_2$, a to je tvrdnja Propozicije 6 za koju smo pokazali da vrijedi.

PRETPOSTAVKA:
Pretpostavimo da tvrdnja vrijedi za $n = k$, tj. da ako $p|a_1a_2\cdots a_k$, onda $p|a_i$ za neki $i \in \{1, 2, \ldots, k\}$.

KORAK:
Pokažimo da tvrdnja vrijedi za $n = k+1$, tj. da ako $p|a_1\cdots a_ka_{k+1}$, onda $p|a_i$ za neki $i \in \{1, \ldots, k, k+1\}$. Kako $p|a_1\cdots a_ka_{k+1}$, to možemo zapisati kao $p|(a_1\cdots a_k)a_{k+1}$. Primjenom Propozicije 6 vrijedi da $p|a_1\cdots a_k$ ili $p|a_{k+1}$. Iz $p|a_1\cdots a_k$ zbog pretpostavke indukcije znamo da $p|a_i$ za neki indeks $i \in \{1, 2, \ldots, k\}$ pa smo time pokazali da $p|a_i$ za neki $i \in \{1, \ldots, k, k+1\}$. □

Korolar 4 (vidi [17]). *Ako su $p, q_1, q_2, \ldots, q_n$ prosti brojevi i $p|q_1q_2\ldots q_n$, onda je $p = q_k$ za neki k, $1 \leq k \leq n$.*

Dokaz. Pretpostavimo da su $p, q_1, q_2, \ldots, q_n$ prosti brojevi i da $p|q_1q_2\cdots q_n$. Zbog Korolara 3 znamo da $p|q_k$ za neki k, $1 \leq k \leq n$. Kako je q_k prost, jedini pozitivni djelitelji su mu 1 i q_k. S obzirom na to da je $p > 1$ slijedi da je $p = q_k$. □

Teorem 7 (Osnovni teorem aritmetike, vidi [6]). *Svaki se prirodan broj veći od 1 može prikazati kao produkt potencija prostih faktora. Taj prikaz jedinstven je do na poredak faktora.*

Dokaz. Dokažimo prvo egzistenciju ovakve faktorizacije. Neka je $n \in \mathbb{N}, n > 1$. Ako je n prost broj, onda smo gotovi. Ako je n složen, onda $\exists d \in \mathbb{N} : d|n$ i $1 < d < n$. Među svim takvim djeliteljima broja n odaberimo najmanji i označimo ga s p_1. To je moguće napraviti zbog principa dobre uređenosti skupa $\mathbb{N}$[1]. Zaključujemo da p_1 mora biti prost broj jer bi u suprotnom $\exists q \in \mathbb{N} : q|p_1$ i $1 < q < p_1$, ali onda bi iz $q|p_1$ i $p_1|n$, prema iv) dijelu Teorema 1, slijedilo da $q|n$, a to je u kontradikciji s odabirom broja p_1 kao najmanjeg djelitelja od n različitog od 1. Sada n možemo zapisati u obliku

$$n = p_1n_1,$$

pri čemu je p_1 prost broj i $1 < n_1 < n$. Ako je n_1 prost, onda smo n zapisali kao produkt prostih faktora. Ako je n_1 složen, onda nastavljamo s postupkom, tj. pronalazimo prost broj p_2 takav da $n_1 = p_2n_2$ i $1 < n_2 < n_1$. Sada je

$$n = p_1p_2n_2.$$

[1] **Princip dobre uređenosti skupa $\mathbb{N}$:** Svaki neprazan podskup S skupa $\mathbb{N}$ sadrži najmanji element, tj. $\exists a \in S : a \leq b, \forall b \in S$.

Ako je n_2 prost broj, tu stajemo. Ako nije, pronalazimo prost broj p_3 takav da $n_2 = p_3 n_3$ i $1 < n_3 < n_2$ i dobivamo:

$$n = p_1 p_2 p_3 n_3.$$

Niz $n > n_1 > n_2 > \cdots > 1$ padajući je i konačan (jer n ima konačno mnogo prostih djelitelja) pa će nakon konačno mnogo koraka n_{k-1} biti prost i označimo ga s p_k. To nam daje traženi zapis broja n kao produkta prostih faktora, tj.

$$n = p_1 p_2 \cdots p_k.$$

Preostalo je još dokazati jedinstvenost faktorizacije (do na poredak faktora). Pretpostavimo suprotno, tj. da n nema jedinstvenu faktorizaciju. Neka su

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l, \ k \leq l,$$

dvije faktorizacije broja n, pri čemu su p_i, q_j prosti brojevi, $\forall i \in \{1, \ldots, k\}, \forall j \in \{1, \ldots, l\}$, takvi da

$$p_1 \leq p_2 \leq \cdots \leq p_k \quad \text{i} \quad q_1 \leq q_2 \leq \cdots \leq q_l.$$

Zbog toga što $p_1 | q_1 q_2 \cdots q_l$, prema Korolaru 4, slijedi da je $p_1 = q_j$ za neki $j \in \{1, \ldots, l\}$, ali onda je i $p_1 \geq q_1$. Analogno razmatranje daje $q_1 \geq p_1$ pa zaključujemo da je $p_1 = q_1$. Sada obje strane jednakosti možemo podijeliti sa zajedničkim faktorom i dobivamo:

$$p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_l.$$

Ponovimo isti proces kao i ranije te dobivamo da je $p_2 = q_2$. Tada ponovnim dijeljenjem jednakosti sa zajedničkim faktorom imamo:

$$p_3 p_4 \cdots p_k = q_3 q_4 \cdots q_l.$$

Dalje provodimo isti postupak. Kada bi vrijedila nejednakost $k < l$, onda bi u jednom koraku dobili sljedeće:

$$1 = q_{k+1} q_{k+2} \cdots q_l,$$

što nije moguće jer je svaki $q_j > 1, j \in \{1, \ldots, l\}$. Stoga je $k = l$ i

$$p_1 = q_1, \quad p_2 = q_2, \quad \ldots, \quad p_k = q_k.$$

Time smo dokazali da su početne faktorizacije međusobno jednake. □

Dakle, svaki se prirodan broj $n > 1$ može zapisati na sljedeći način:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}, \tag{2.1}$$

pri čemu su p_i međusobno različiti prosti brojevi, a $\alpha_i \in \mathbb{N}, i \in \{1, 2, \ldots n\}$. Zapis (2.1) naziva se rastav ili dekompozicija broja n na proste faktore.

Odgovor na pitanje koliko prostih brojeva ima dao je Euklid u devetoj knjizi svojih *Elemenata*:

Teorem 8 (Euklidov teorem, vidi [6]). *Postoji beskonačno mnogo prostih brojeva.*

Dokaz. Dokaz provodimo kontradikcijom. Pretpostavimo da postoji konačno mnogo prostih brojeva. Neka su $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots$ prosti brojevi poredani uzlazno. Označimo s p_n posljednji i najveći prost broj. Pogledajmo sada prirodan broj

$$n = p_1 p_2 \cdots p_n + 1.$$

Kako je $n > 1$, prema Teoremu 7, on je djeljiv nekim prostim brojem p. No, s obzirom na to da su $p_1, p_2, \ldots, p_n$ jedini prosti brojevi, p mora biti jednak jednom od njih. Kako vrijedi da $p|p_1 p_2 \cdots p_n$ i $p|n$, prema dijelu vii) Teorema 1, slijedi da $p|n - p_1 p_2 \cdots p_n$, odnosno $p|1$. Jedini prirodan broj koji zadovoljava to svojstvo je broj 1, a kako je $p > 1$ imamo kontradikciju. Dakle, postoji beskonačno mnogo prostih brojeva. □

Uočimo da u dokazu prethodnoga teorema broj $n = p_1 p_2 \cdots p_n + 1$ nije nužno prost, nego samo ima djelitelja koji je prost i različit od $p_1, p_2, \ldots, p_n$.

Definicija 11 (vidi [17]). *Neka je $x \in \mathbb{R}$. Funkcija najveće cijelo ili funkcija "pod", u oznaci $\lfloor x \rfloor$, najveći je cijeli broj koji je manji ili jednak od x, tj.*

$$\lfloor x \rfloor = \max\{n : n \leq x, n \in \mathbb{Z}\}.$$

Propozicija 7 (vidi [17]). *Ako je $n > 1$ složen broj, onda postoji djelitelj d od n takav da je $1 < d \leq \lfloor \sqrt{n} \rfloor$.*

Dokaz. Neka je n složen broj. Tada postoje $d_1, d_2 \in \mathbb{N}$, $1 < d_1, d_2 < n$, takvi da je $n = d_1 d_2$.
Pretpostavimo da je $d_1 > \lfloor \sqrt{n} \rfloor$. Kako je $d_1 \in \mathbb{N}$, onda je $d_1 > \sqrt{n}$. Vrijedi:

$$d_2 = \frac{n}{d_1} < \frac{n}{\sqrt{n}} = \sqrt{n},$$

pri čemu nejednakost slijedi iz:

$$y > x > 0 \Rightarrow \frac{1}{y} < \frac{1}{x}.$$

Dakle, $d_2 < \sqrt{n}$, a kako je $d_2 \in \mathbb{N}$, onda je $d_2 \leq \lfloor \sqrt{n} \rfloor$. Time smo pokazali tvrdnju. □

Sljedeći korolar omogućava skraćivanje procesa pronalaska djelitelja broja n ograničavajući provjeru djelitelja na proste brojeve:

Korolar 5 (vidi [17]). *Ako je $n > 1$ složen, onda ima prostog djelitelja p takvog da je $p \leq \sqrt{n}$.*

Dokaz. Kako je n složen, prema Propoziciji 7 postoji djelitelj $d|n$ takav da je $1 < d \leq \lfloor \sqrt{n} \rfloor$. Nadalje, iz Teorema 7 za $d > 1$ znamo da postoji prosti broj p takav da $p|d$. Kako $p|d$ i $d|n$, slijedi da $p|n$ i $p \leq d$ pa je onda $p \leq \lfloor \sqrt{n} \rfloor$. □

Starogrčki matematičar **Eratosten** (oko 276. pr. Kr. – 194. pr. Kr.) razvio je učinkoviti algoritam za pronalaženje svih prostih brojeva koji su manji ili jednaki nekom broju n. Njemu u čast algoritam je dobio naziv **Eratostenovo sito**. Provodi se na sljedeći način:
Napravimo niz brojeva od 2 do n:

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, \ldots, n.$$

Počevši od 2, koji je prvi prost broj, iz niza izbacujemo sve njegove viškratnike $2m$ takve da je $2 < 2m \leq n$ i dobivamo novi niz:

$$2, 3, 5, 7, 9, 11, 13, 15, 17, 19, \ldots, n.$$

Sljedeći broj u nizu je 3. On je prost pa iz novoga niza izbacujemo sve njegove višekratnike $3m$ takve da je $3 < 3m \leq n$ i dobivamo niz:

$$2, 3, 5, 7, 11, 13, 17, 19, \ldots, n.$$

Općenito, u k-tom koraku niz izgleda ovako:

$$2, 3, 5, 7, 11, 13, 17, 19, \ldots, p, \ldots, n,$$

pri čemu je p k-ti prost broj. Tada iz niza izbacujemo sve višekratnike pm od p takve da je $p < pm \leq n$.
Postupak nastavljamo sve dok ne iscrpimo sve proste brojeve manje ili jednake n. Uočimo da je svaki izbačeni broj iz niza složen, a oni koji su preostali u nizu prosti su. Postupak je dovoljno provoditi do k-toga koraka, gdje, ako je p k-ti prost broj, vrijedi da je $p \leq \sqrt{n}$ (prema Korolaru 5).

Primjer 2. *Pomoću Eratostenovog sita odredimo sve proste brojeve manje ili jednake od* 118.

Rješenje. Prvo napravimo tablicu s brojevima od 2 do 118:

2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37
38	39	40	41	42	43	44	45	46
47	48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63	64
65	66	67	68	69	70	71	72	73
74	75	76	77	78	79	80	81	82
83	84	85	86	87	88	89	90	91
92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109
110	111	112	113	114	115	116	117	118

Primijetimo da ćemo redom izbacivati višekratnike prostih brojeva p za koje vrijedi

$$p \leq \lfloor \sqrt{118} \rfloor = 10, \text{ tj. } p^2 \leq 118.$$

Posljednji prost broj za koji to vrijedi je broj 7 (za 11 je $11^2 = 121 > 118$).

1. Krećemo od broja 2 i precrtavamo sve njegove višekratnike.

2. Prvi neprecrtani broj nakon broja 2 je 3 pa izbacujemo sve njegove višekratnike.

3. Sljedeći je broj 5 pa precrtavamo sve njegove višekratnike.

4. Nakon broja 5, prvi neprecrtani broj je 7. On je posljednji prost broj čije ćemo višekratnike precrtati.

Konačno, dobivamo sljedeću tablicu:

2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19
~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~
29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37
~~38~~	~~39~~	~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~
47	~~48~~	~~49~~	~~50~~	51	~~52~~	53	~~54~~	~~55~~
~~56~~	~~57~~	~~58~~	59	~~60~~	61	~~62~~	~~63~~	~~64~~
~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~	71	~~72~~	73
~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~	~~81~~	~~82~~
83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~	~~91~~
~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109
~~110~~	~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~

Svi precrtani brojevi u tablici složeni su, a preostali su brojevi prosti.

2.2 Prosti brojevi posebnoga oblika

U teoriji brojeva možemo pronaći razne brojeve čiji zapisi imaju poseban oblik, a ovo se poglavlje bavi samo trima takvima. Neki od njih, upravo zbog svojega oblika, koriste se u testovima prostosti o kojima ćemo nešto više reći u nastavku rada.

2.2.1 Fermatovi prosti brojevi

Pierre de Fermat (1601. – 1655.) bio je francuski pravnik koji je, iako se matematikom bavio u svoje slobodno vrijeme, jedan od najpoznatijih matematičara 17. stoljeća. Smatra se suosnivačem analitičke geometrije i teorije vjerojatnosti te prethodnikom infinitezimalnoga računa, a njegovi su doprinosi teoriji brojeva najznačajniji ([5]).

Definicija 12. *Broj oblika* $F_n = 2^{2^n} + 1, n \in \mathbb{N}_0$, *naziva se Fermatov broj. Fermatov broj* F_n *koji je prost naziva se Fermatov prost broj.*

Iako je Fermat u svojemu pismu Mersenneu pretpostavio da su svi brojevi oblika $F_n = 2^{2^n} + 1$ prosti i pokazao da to vrijedi za $n = 0, 1, 2, 3, 4$, stotinjak godina kasnije švicarski matematičar **Leonhard Euler** (1707. – 1983.) opovrgnuo je tu tvrdnju pokazavši da $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4\,294\,967\,297$ nije prost broj jer $641 | F_5$. Danas je poznato samo prvih, a možda i jedinih, pet Fermatovih prostih brojeva. Postoji li ih beskonačno mnogo ili ne, jedna je od još uvijek nedokazanih tvrdnji u teoriji brojeva.

n	F_n
0	3
1	5
2	17
3	257
4	65 537

Tablica 2.1: Tablica svih poznatih Fermatovih prostih brojeva

Sljedeći propozicija daje nam neka svojstva Fermatovih brojeva:

Propozicija 8 (vidi[19])**.** *Za* $F_n = 2^{2^n} + 1$ *vrijedi sljedeće:*

i) $F_n = (F_{n-1} - 1)^2 + 1$, *za* $n \geq 1$;

ii) $F_n = F_0 \cdots F_{n-1} + 2$, *za* $n \geq 1$;

iii) $F_n = F_{n-1}^2 - 2(F_{n-2} - 1)^2$, *za* $n \geq 2$;

iv) $F_n = F_{n-1} + 2^{2^{n-1}} F_0 \cdots F_{n-2}$, *za* $n \geq 2$.

Propozicija 9 (vidi [14])**.** *Svaka su dva različita Fermatova broja relativno prosta, tj.* $(F_i, F_j) = 1$, *za* $i \neq j$.

2.2.2 Mersenneovi prosti brojevi

Marin Mersenne (1588. – 1648.) bio je francuski redovnik koji je oko sebe okupljao najbitnije matematičare toga doba i osigurao komunikaciju i razmjenu ideja među njima. U teoriji brojeva bavio se savršenim i prostim brojevima ([5]), a u ovome poglavlju definirat ćemo ih te vidjeti poveznicu među njima. Također, vidjet ćemo i kojega su oblika prosti faktori Mersenneovih složenih brojeva.

Definicija 13. *Broj oblika* $M_n = 2^n - 1, n \in \mathbb{N}$, *naziva se Mersenneov broj. Mersenneov broj* M_n *koji je prost naziva se Mersenneov prost broj.*

n	M_n
2	3
3	7
5	31
7	127
13	8191

Tablica 2.2: Tablica prvih pet Mersenneovih prostih brojeva

Do danas je poznato ukupno 51 Mersenneovih prostih brojeva. Posljednji je otkriven 2018. godine i to je $M_{82\,589\,933} = 2^{82\,589\,933} - 1$ koji ima 24 862 048 znamenki i trenutno je najveći poznati prost broj. Iako se sluti da Mersenneovih prostih brojeva ima beskonačno mnogo, ta tvrdnja još uvijek nije dokazana. Tablica svih otkrivenih Mersenneovih prostih brojeva može se pogledati na internetskoj stranici: GIMPS.

Iz Tablice 2.2 uočavamo da je svaki od indeksa n prost broj, a poveznica između Mersenneovih prostih brojeva M_n i indeksa n koji je prost broj dana je sljedećom propozicijom:

Propozicija 10 (vidi [14]). *Ako je $M_n = 2^n - 1$ prost, onda je i n prost broj.*

Dokaz. Dokaz provodimo obratom po kontrapoziciji, tj. pokazat ćemo da ako je n složen broj, onda je i M_n složen.
Ako je n složen broj, onda se može zapisati u obliku $n = rs$, za neke $r, s \in \mathbb{N} \setminus \{1\}$. Tada je

$$2^n - 1 = 2^{rs} - 1 = (2^s)^r - 1^r = (2^s - 1)(2^{s(r-1)} + 2^{s(r-2)} + \cdots + 2^s + 1),$$

a onda je i M_n složen jer $2^s - 1 | M_n$ i $1 < 2^s - 1 < M_n$. □

Uočimo da obrat prethodne propozicije ne vrijedi, tj. ukoliko je n prost broj, M_n ne mora biti prost:

Primjer 3. *Znamo da je $n = 11$ prost broj, ali $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ nije prost broj.*

Prisjetimo se definicije savršenih brojeva i pogledajmo poveznicu s Mersenneovim prostim brojevima:

Definicija 14. *Za broj $n \in \mathbb{N}$ kažemo da je savršen ako je suma svih njegovih pravih djelitelja jednaka n, tj. ako je $\sum_{d_i | n} d_i = n, 1 \leq d_i < n$.*

Primjer 4. *Prva tri savršena broja su:*

- $6 = 1 + 2 + 3$;
- $28 = 1 + 2 + 4 + 7 + 14$;

- $496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248.$

Do sada je poznato 51 savršenih brojeva i oni su svi parni. Na pitanje o postojanju neparnih savršenih brojeva još uvijek nije dan odgovor.

Karakterizacije savršenih i prostih brojeva pomoću funkcije σ dane su u sljedećim propozicijama:

Propozicija 11 (vidi [17]). *Broj n je savršen ako i samo ako je $\sigma(n) = 2n$.*

Dokaz.

$\Longrightarrow$ Neka je n savršen broj i neka su $d_1, \ldots, d_k$ svi njegovi pravi djelitelji. Ne zaboravimo da i $n|n$. Imamo:

$$\sigma(n) = \underbrace{d_1 + \cdots + d_k}_{= n,\ n \text{ savršen}} + n = n + n = 2n.$$

$\Longleftarrow$ Neka je $\sigma(n) = 2n$ i neka su $d_1, d_2, \ldots, d_k$ svi pozitivni djelitelji broja n. Kako $n|n$, stavimo da je $d_k = n$. Vrijedi sljedeće:

$$\sigma(n) = \sum_{i=1}^{k} d_i = \sum_{i=1}^{k-1} d_i + n.$$

Označimo sa $S = \sum_{i=1}^{k-1} d_i$ sumu svih pravih djelitelja od n. Kako je $\sigma(n) = 2n$, vrijedi:

$$S + n = 2n \quad \Longrightarrow \quad S = 2n - n = n.$$

Dakle, dobili smo da je suma svih pravih djelitelja od n jednaka n pa je broj n savršen.

□

Propozicija 12 (vidi [17]). *Broj p je prost ako i samo ako je $\sigma(p) = 1 + p$.*

Dokaz.

$\Longrightarrow$ Neka je p prost broj. Znamo da on onda ima samo dva pozitivna djelitelja 1 i p. Dakle, $\sigma(p) = 1 + p$.

$\Longleftarrow$ Neka za broj p vrijedi da je $\sigma(p) = 1 + p$. Kada bi p bio složen broj i $d_1, \ldots, d_k$ svi djelitelji od p takvi da $1 < d_i < p, 1 \leq i \leq k$, onda bi vrijedilo:

$$\sigma(p) = 1 + d_1 + \cdots + d_k + p,$$

a to bi značilo da je $\sigma(p) > 1 + p$ što je u kontradikciji s pretpostavkom. Dakle, 1 i p jedini su djelitelji broja p pa je p prost broj.

□

Poveznicu između Mersenneovih prostih brojeva i savršenih brojeva poznavali su još starogrčki matematičari. Euklid je pokazao da vrijedi sljedeće:

Teorem 9 (vidi [17]). *Ako je $M_k = 2^k - 1$ Mersenneov prost broj, onda je $2^{k-1}(2^k - 1)$ paran savršen broj.*

Dokaz. U dokazu ćemo koristiti formulu za sumu prvih n članova geometrijskoga niza:

$$a + ar + ar^2 + \cdots + ar^{n-1} = \sum_{i=0}^{n-1} ar^i = \frac{a(1-r^n)}{1-r}. \tag{2.2}$$

Pretpostavimo da je $2^k - 1$ prost broj. Pravi djelitelji broja $N = 2^{k-1}(2^k - 1)$ su:

$$\underbrace{1, 2, 2^2, \ldots, 2^{k-2}, 2^{k-1}}_{\text{1. dio}}, \underbrace{2^k - 1, 2(2^k - 1), 2^2(2^k - 1), \ldots, 2^{k-2}(2^k - 1)}_{\text{2. dio}}. \tag{2.3}$$

Sumiramo li elemente 1. dijela niza (2.3) primjećujemo da imamo sumu prvih k članova geometrijskoga niza pa primjenjujemo formulu (2.2) za $a = 1, r = 2$ i $n = k$ i dobivamo:

$$\sum_{i=0}^{k-1} 2^i = \frac{1(1-2^k)}{1-2} = 2^k - 1. \tag{2.4}$$

Sumiramo li sada 2. dio niza (2.3) dobivamo:

$$\sum_{j=0}^{k-2} 2^j(2^k - 1) = (2^k - 1) \sum_{j=0}^{k-2} 2^j, \tag{2.5}$$

a primjenom formule (2.2) na sumu s desne strane prethodne jednakosti, za $a = 1, r = 2$ i $n = k - 1$, imamo:

$$\sum_{j=0}^{k-2} 2^j = \frac{1(1-2^{k-1})}{1-2} = 2^{k-1} - 1. \tag{2.6}$$

Uvrstimo li (2.6) u (2.5) dobivamo:

$$\sum_{j=0}^{k-2} 2^j(2^k - 1) = (2^k - 1)(2^{k-1} - 1). \tag{2.7}$$

Konačno, zbrajanjem jednakosti (2.4) i (2.7) dobivamo sumu svih pravih djelitelja od N:

$$\begin{aligned} \sum_{i=0}^{k-1} 2^i + \sum_{j=0}^{k-2} 2^j(2^k - 1) &= (2^k - 1) + (2^k - 1)(2^{k-1} - 1) \\ &= (2^k - 1)(1 + 2^{k-1} - 1) \\ &= 2^{k-1}(2^k - 1) \\ &= N. \end{aligned} \tag{2.8}$$

Time smo pokazali da je broj N savršen. □

Nakon otprilike 2000 godina Euler je pokazao da vrijedi i obrat prethodnoga teorema:

Teorem 10 (vidi [20]). *Svaki je paran savršen broj oblika* $2^{k-1}(2^k-1)$, *pri čemu je* 2^k-1 *Mersenneov prost broj.*

Dokaz. Neka je $N = 2^{k-1}(2^k-1)$ paran savršen broj. Zapišimo ga u sljedećem obliku:

$$N = 2^{k-1}m,$$

pri čemu je $k \geq 2$ i m neparan. S obzirom na to da je N savršen vrijedi:

$$\sigma(N) = 2N = 2^k m. \tag{2.9}$$

Kako je funkcija σ multiplikativna i $(2^{k-1}, m) = 1$ vrijedi:

$$\sigma(N) = \sigma(2^{k-1}m) = \sigma(2^{k-1})\sigma(m) = (2^k-1)\sigma(m). \tag{2.10}$$

Iz jednakosti (2.9) i (2.10) slijedi da je

$$2^k m = (2^k-1)\sigma(m). \tag{2.11}$$

Neka je

$$\sigma(m) = m + t,$$

gdje je t suma svih pravih djelitelja od m. Uvrstimo li prethodnu jednakost u (2.11) dobivamo sljedeće:

$$2^k m = (2^k-1)(m+t), \text{ tj.}$$
$$m = (2^k-1)t.$$

Prema tome, $t|m$ i t mora biti jedan od pravih djelitelja od m što je moguće jedino u slučaju kada je $t = 1$. Dakle, $\sigma(m) = m+1$ pa je $m = 2^k-1$ prost broj. □

U nastavku ćemo se baviti djeliteljima Mersenneovih složenih brojeva.

Propozicija 13 (vidi [17]). *Neka je* p *prost broj. Vrijedi:*

i) Ako je $ab \equiv 0 \pmod{p}$, *onda je* $a \equiv 0 \pmod{p}$ *ili* $b \equiv 0 \pmod{p}$.

ii) $a^2 \equiv b^2 \pmod{p}$ *ako i samo ako je* $a \equiv \pm b \pmod{p}$.

Dokaz.

i) Neka je $ab \equiv 0 \pmod{p}$. To znači da $p|ab$, a kako je p prost broj, prema Propoziciji 6, vrijedi da $p|a$ ili $p|b$, tj. $a \equiv 0 \pmod{p}$ ili $b \equiv 0 \pmod{p}$.

ii)

$\Longrightarrow$ Neka je $a^2 \equiv b^2 \pmod{p}$. To znači da $p|a^2-b^2 = (a-b)(a+b)$. Kako je p prost broj takav da $p|(a-b)(a+b)$, prema Propoziciji 6 $p|a-b$ ili $p|a+b$, tj. $a \equiv b \pmod{p}$ ili $a \equiv -b \pmod{p}$.

$\Longleftarrow$ Neka je $a \equiv \pm b \pmod{p}$. Treba pokazati da je $a^2 \equiv b^2 \pmod{p}$.

1° Neka je $a \equiv b \pmod{p}$. Tada postoji $k \in \mathbb{Z}$ takav da je $a = b + kp$. Kvadriranjem dobivamo da je $a^2 = b^2 + 2bkp + k^2p^2$. Kako $p|(2bkp + k^2p^2) = p(2bk + k^2p)$, vrijedi da je $a^2 \equiv b^2 \pmod{p}$.

2° Neka je $a \equiv -b \pmod{p}$. Tada postoji $k \in \mathbb{Z}$ takav da je $a = -b + kp$. Kvadriranjem dobivamo da je $a^2 = b^2 - 2bkp + k^2p^2$. Kako $p|(-2bkp + k^2p^2) = p(-2bk + k^2p)$, vrijedi da je $a^2 \equiv b^2 \pmod{p}$.

□

Lema 2 (vidi [17]). *Neka je p prost broj. Vrijedi:*

$$x^2 \equiv 1 \pmod{p} \iff x \equiv \pm 1 \pmod{p}.$$

Dokaz. Iz dijela ii) Propozicije 13 za $a = x$ i $b = 1$ slijedi tvrdnja. □

Za dokaz malog Fermatovog teorema potrebna nam je karakterizacija prostih brojeva pomoću Eulerove funkcije φ:

Propozicija 14 (vidi [17]). *Broj p je prost ako i samo ako je $\varphi(p) = p - 1$.*

Dokaz.

$\Longrightarrow$ Neka je p prost broj. Tada za svaki $1 \leq n \leq p - 1$ vrijedi da je $(p, n) = 1$. Takvih brojeva ima ukupno $p - 1$ pa je $\varphi(p) = p - 1$.

$\Longleftarrow$ Neka je $\varphi(p) = p - 1$. To znači da je broj p relativno prost s $p - 1$ brojeva, tj. za svaki $1 \leq n \leq p - 1$ je $(p, n) = 1$ pa je p prost broj.

□

Teorem 11 (Mali Fermatov teorem, vidi [17]). *Neka je p prost broj i $a \in \mathbb{Z}$. Tada je $a^p \equiv a \pmod{p}$ te ako $p \nmid a$, vrijedi i $a^{p-1} \equiv 1 \pmod{p}$.*

Dokaz. Neka je p prost broj takav da $p \nmid a$. Tada je $(p, a) = 1$. Prema Teoremu 6 je $a^{\varphi(p)} \equiv 1 \pmod{p}$. Iz Propozicije 14 slijedi da je $\varphi(p) = p - 1$. Dakle,

$$a^{\varphi(p)} \equiv a^{p-1} \equiv 1 \pmod{p}.$$

Prema Korolaru 1, pomnožimo li prethodnu kongruenciju s a dobivamo da je $a^p \equiv a \pmod{p}$. Prethodna kongruencija vrijedi i kada $p|a$ jer je tada $a \equiv 0 \equiv a^p \pmod{p}$. □

Propozicija 15. *Neka je $n \in \mathbb{N}$ i $p = 2n + 1$ neparan prost broj. Tada ili $p|2^n - 1$ ili $p|2^n + 1$.*

Dokaz. Neka je $n \in \mathbb{N}$ i $p = 2n + 1$ neparan prost broj. Treba pokazati da p dijeli $2^n - 1$ ili $2^n + 1$, tj. u terminima kongruencija da je $2^n \equiv 1 \pmod{p}$ ili $2^n \equiv -1 \pmod{p}$, redom. S obzirom na to da je p prost broj, primjenom Teorema 11 za $a = 2$ dobivamo:

$$2^{p-1} \equiv 1 \pmod{p}. \tag{2.12}$$

Kako je $p = 2n + 1$, to implicira da je $p - 1 = 2n$. Uvrštavanjem prethodnoga u (2.12) dobivamo sljedeće:

$$2^{p-1} \equiv 2^{2n} \equiv (2^n)^2 \equiv 1 \pmod{p}.$$

Primjenom Leme 2 za $x = 2^n$ dobivamo:

$$2^n \equiv \pm 1 \pmod{p}.$$

Preostaje još pokazati da p ne dijeli oba $2^n - 1$ i $2^n + 1$. Pretpostavimo suprotno, tj. da p dijeli oba. Tada, prema dijelu vii) Teorema 1, $p|(2^n + 1) - (2^n - 1) = 2$ što je nemoguće jer je p neparan prost broj. Dakle, p će uvijek dijeliti samo jednog od $2^n - 1$ i $2^n + 1$. □

Primjer 5. *Primijenimo prethodnu propoziciju za $n = 3$ i $n = 5$.*

Rješenje.

i) Za $n = 3$ je $p = 2n + 1 = 2 \cdot 3 + 1 = 7$ prost broj. Prema prethodnoj propoziciji $p|2^n - 1$ ili $p|2^n + 1$.

$$7|2^3 - 1 = 7 \quad \text{i} \quad 7 \nmid 2^3 + 1 = 9.$$

Dakle, $7|2^n - 1$.

ii) Za $n = 5$ je $p = 2n + 1 = 11$ prost broj. Prema prethodnoj propoziciji $p|2^n - 1$ ili $p|2^n + 1$.

$$11 \nmid 2^5 - 1 = 31 \quad \text{i} \quad 11|2^5 + 1 = 33.$$

Dakle, $11|2^n + 1$.

Kako bismo dokazali sljedeću propoziciju, potrebne su nam definicije i tvrdnje vezane uz kvadratne ostatke:

Definicija 15. *Neka je $n \in \mathbb{N}$. Za $a \in \mathbb{Z}$ takav da je $(a, n) = 1$ kažemo da je kvadratni ostatak modulo n ako postoji $x \in \mathbb{Z}$ koji zadovoljava kongruenciju $x^2 \equiv a \pmod{n}$. U slučaju da takav x ne postoji, onda kažemo da je a kvadratni neostatak modulo n.*

Teorem 12 (Eulerov kriterij, vidi [17])**.** *Za neparan prost broj p i $a \in \mathbb{Z}$ takav da $p \nmid a$ vrijedi:*

$$a \text{ je kvadratni ostatak modulo } p \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Definicija 16. *Neka je p neparan prost broj i $a \in \mathbb{Z}$. Legedreov simbol $\left(\frac{a}{p}\right)$ definiran je na sljedeći način:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ ako je kvadratni ostatak modulo } p \\ -1, & a \text{ ako je kvadratni neostatak modulo } p \\ 0, & a \equiv 0 \pmod{p} \end{cases}.$$

Propozicija 16 (vidi [17]). *Neka je p neparan prost broj i $a \in \mathbb{Z}$. Tada je*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Propozicija 17 (vidi [17]). *Neka je p neparan prost broj. Tada vrijedi:*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod 8 \\ -1, & p \equiv \pm 3 \pmod 8 \end{cases}.$$

Propozicija 18 (vidi [17]). *Neka je $p = 2n + 1$ prost broj. Vrijedi sljedeće:*

i) Ako je $p \equiv \pm 1 \pmod 8$, onda $p | 2^n - 1$.

ii) Ako je $p \equiv \pm 3 \pmod 8$, onda $p | 2^n + 1$.

Dokaz.

i) Neka je $p \equiv \pm 1 \pmod 8$. Zbog Propozicije 17 znamo da je onda 2 kvadratni ostatak modulo p. Trebamo pokazati da je $2^n \equiv 1 \pmod p$. Primjenom Teorema 12 za $a = 2$ znamo:

$$2 \text{ je kvadratni ostatak modulo } p \iff 2^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

Kako je $p = 2n + 1$, onda je $n = \frac{p-1}{2}$ pa je

$$2^{\frac{p-1}{2}} = 2^n \equiv 1 \pmod p,$$

a iz toga slijedi da $p | 2^n - 1$.

ii) Neka je $p \equiv \pm 3 \pmod 8$. Zbog Propozicije 17 znamo da je 2 kvadratni neostatak modulo p. Trebamo pokazati da je $2^n \equiv -1 \pmod p$. Primjenom Teorema 12 za $a = 2$ znamo:

$$2 \text{ je kvadratni neostatak modulo } p \iff 2^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

Kako je $p = 2n + 1$, onda je $n = \frac{p-1}{2}$ pa je

$$2^{\frac{p-1}{2}} = 2^n \equiv -1 \pmod p,$$

a iz toga slijedi da $p | 2^n + 1$.

□

2.2.3 Prosti brojevi Sophie Germain

Sophie Germain (1776. – 1831.) bila je revolucionarna samouka francuska matematičarka čija su najznačajnija postignuća u teoriji elastičnosti i teoriji brojeva. U ovome poglavlju definirat ćemo proste brojeve koji su dobili ime njoj u čast i vidjeti njihovu važnost u pronalasku prostih djelitelja Mersenneovih složenih brojeva.

Definicija 17. *Ako je q prost broj takav da je i $p = 2q + 1$ prost, onda se q naziva Sophieinim prostim brojem, a broj p sigurnim prostim brojem.*

q	$p = 2q + 1$
2	5
3	7
5	11
11	23
23	47

Tablica 2.3: Tablica prvih pet Sophieinih i sigurnih prostih brojeva

Kao i kod Fermatovih i Mersenneovih prostih brojeva, slutnja o postojanju beskonačno mnogo Sophieinih prostih brojeva još uvijek nije dokazana.
U veljači 2016. godine pronađen je trenutno najveći Sophiein prost broj $q = 2\,618\,163\,402\,417 \cdot 2^{1\,290\,000} - 1$ koji ima 388 342 znamenke, a u svibnju 2024. godine pronađen je novi Sophiein prost broj $q = 21\,480\,284\,945\,595 \cdot 2^{333\,443} - 1$ koji ima 100 390 znamenki.

Propozicija 19 (vidi [17])**.** *Neka su q i $p = 2q + 1$ prosti brojevi.*

i) Ako je $q \equiv -1 \pmod 4$, onda $p|2^q - 1$.

ii) Ako je $q \equiv 1 \pmod 4$, onda $p|2^q + 1$.

Dokaz. Neka su q i $p = 2q + 1$ prosti brojevi.

i) Neka je $q \equiv -1 \pmod 4$. Tada se on može zapisati kao $q = 4k - 1, k \in \mathbb{Z}$. Vrijedi da je

$$p = 2(4k - 1) + 1 = 8k - 1 \equiv -1 \pmod 8,$$

a prema dijelu i) Propozicije 18 slijedi da $p|2^q - 1$.

ii) Neka je $q \equiv 1 \pmod 4$. Tada se on može zapisati kao $q = 4k + 1, k \in \mathbb{Z}$. Vrijedi da je

$$p = 2(4k + 1) + 1 = 8k + 3 \equiv 3 \pmod 8,$$

a prema dijelu ii) Propozicije 18 slijedi da $p|2^q + 1$.

□

Propozicija 20 (vidi [17]). *Ako je $q \neq 3$ Sophiein prost broj i $q \equiv -1 \pmod 4$, onda je Mersenneov broj $M_q = 2^q - 1$ složen i $p|2^q - 1$, gdje je $p = 2q + 1$.*

Dokaz. Neka je $q \neq 3$ Sophiein prost broj. Tada je i $p = 2q + 1$ prost. Kako je $q \equiv -1 \pmod 4$ prema dijelu i) Propozicije 19 vrijedi da $p|2^q - 1$. Treba pokazati da je $p \neq 2^q - 1$. Pretpostavimo suprotno, tj. da je $p = 2^q - 1$. Znamo da je $p = 2q + 1$. Uvrštavanjem toga u prethodnu jednakost dobivamo da je

$$2^q - 1 = 2q + 1 \quad \Longrightarrow \quad 2^q - 2q = 2 \quad \Longrightarrow \quad 2^{q-1} - q = 1.$$

Stoga je $2^{q-1} = q + 1$, a to nije moguće jer je, kao što ćemo dokazati u nastavku, $2^{q-1} > q + 1, \forall q > 3$.

Metodom matematičke indukcije pokažimo da $\forall n \in \mathbb{N}, n > 3$, vrijedi $2^{n-1} > n + 1$.
BAZA:
Za $n = 4$ je $2^{4-1} = 2^3 = 8 > 4 + 1 = 5$.

PRETPOSTAVKA:
Pretpostavimo da za $n = k$ vrijedi nejednakost $2^{k-1} > k + 1$.

KORAK:
Pokažimo da tvrdnja vrijedi za $n = k + 1$, tj. da je $2^k > k + 2$. Vrijedi sljedeće:

$$2^k = 2 \cdot \underbrace{2^{k-1}}_{> k+1} > 2(k + 1) = 2k + 2 > k + 2.$$

Dakle, $p \neq 2^q - 1$ što znači da je p netrivijalan djelitelj od $M_q = 2^q - 1$ pa je M_q složen broj. □

Prisjetimo se sljedeće definicije i propozicije jer one će nam kasnije trebati:

Definicija 18. *Neka je $n > 1$, $a \in \mathbb{Z}$ i $(a, n) = 1$. Red od a modulo n, u oznaci $ord_n(a)$, najmanji je prirodan broj k za koji je $a^k \equiv 1 \pmod n$.*

Propozicija 21 (vidi [17]). *Neka je k red od a modulo n. Tada vrijedi:*

$$a^h \equiv 1 \pmod n \quad \Longleftrightarrow \quad k|h.$$

Propozicija 22 (vidi [17]). *Neka je q neparan prost broj. Bilo koji prosti djelitelj p Mersenneovog složenog broja $M_q = 2^q - 1$ oblika je $p = 2kq + 1, k \in \mathbb{Z}$.*

Dokaz. Neka je q neparan prost broj. Pretpostavimo da je p prosti djelitelj od $M_q = 2^q - 1$. Treba pokazati da je $p = 2kq + 1$. Kako je $2^q \equiv 1 \pmod p$ i $k \in \mathbb{N}$ je najmanji broj za koji vrijedi da je

$$2^k \equiv 1 \pmod p, \tag{2.13}$$

iz Propozicije 21, uz $a = 2$ i $h = q$, dobivamo da $k|q$. Kako je q prost broj, njegovi jedini pozitivni djelitelji su 1 i q što implicira da je $k = 1$ ili $k = q$.
Pretpostavimo da je $k = 1$. Tada iz (2.13) slijedi da je

$$2^1 = 2 \equiv 1 \pmod p$$

pa $p|2-1=1$, a to ne vrijedi jer je p prost broj. Dakle, $k \neq 1$, tj. $k = q$.
Iz Teorema 11 za $a = 2$ je $2^{p-1} \equiv 1 \pmod{p}$, a primjenom Propozicije 21 za $a = 2, k = q$ i $h = p-1$ slijedi da $q|p-1$. Tada $\exists m \in \mathbb{Z} : p-1 = qm$, tj. $p = qm+1$. Preostaje još pokazati da je broj m paran. Zadano nam je da je q neparan prost broj, a iz činjenice da $p|2^q - 1$ znamo da je i p neparan broj. To implicira da je $p-1$ paran pa onda i qm mora biti paran. Dakle, m je paran. Stavimo da je $m = 2l, l \in \mathbb{Z}$. Tada je

$$p = 2lq + 1.$$

□

Napomena 1. *Ako je za $k = 1$ broj p prost, onda će u prethodnoj propoziciji q biti Sophiein prost broj.*

Propozicija 23. *Neka je q neparan prost broj. Bilo koji prosti djelitelj p složenog Mersenneovog broja $M_q = 2^q - 1$ zadovoljava kongruenciju*

$$p \equiv \pm 1 \pmod{8}.$$

Dokaz. Neka je q neparan prost broj i p prosti djelitelj od $2^q - 1$. Tada je

$$2^q \equiv 1 \pmod{p}. \tag{2.14}$$

Prema Propoziciji 22 znamo da je $p = 2kq + 1$ pa je

$$qk = \frac{p-1}{2}.$$

Potenciramo li kongruenciju (2.14) eksponentom k dobivamo:

$$\begin{gathered}(2^q)^k = 2^{qk} \equiv 1^k \equiv 1 \pmod{p} \\ 2^{qk} = 2^{\frac{p-1}{2}} \equiv 1 \pmod{p}\end{gathered}.$$

Iz Teorema 12 slijedi da je 2 kvadratni ostatak modulo p. Taj zapis pomoću Legendreovog simbola je $\left(\frac{2}{p}\right) = 1$, a iz Propozicije 17 slijedi da je $p \equiv \pm 1 \pmod{8}$. □

2.3 Distribucija prostih brojeva

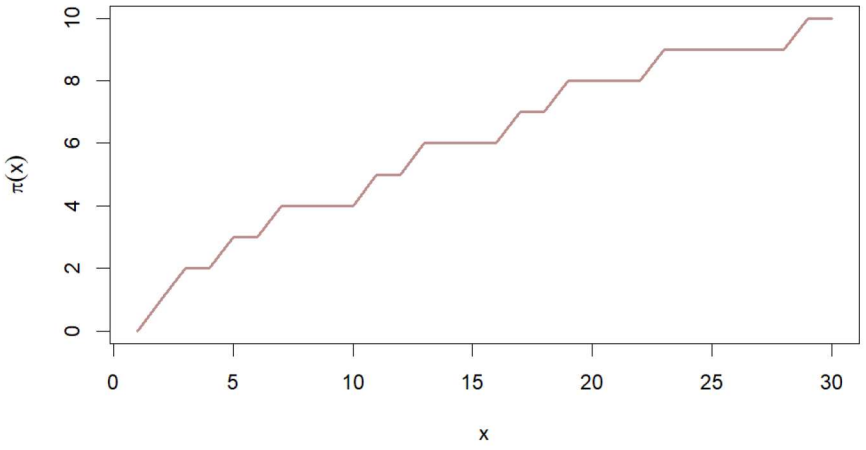
Ranije smo vidjeli da prostih brojeva ima beskonačno mnogo, no još uvijek nije otkrivena formula kojom bismo mogli odrediti sljedeći (novi) prost broj. Iako se na prvi pogled čini da je njihova raspršenost među prirodnim brojevima slučajna, brojni matematičari uočili su kako ipak postoji određena pravilnost u njihovom ponašanju.

Definicija 19. *S $\pi(x)$ označavamo broj prostih brojeva koji su manji ili jendaki prizvoljnom broju $x \in \mathbb{N}$, tj.*

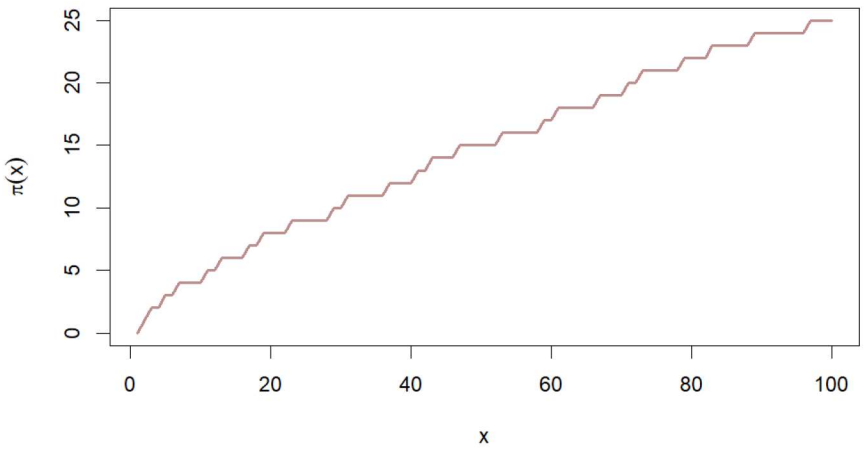
$$\pi(x) = \sum_{p \leq x} 1.$$

Primjer 6. *Odredimo* $\pi(x)$ *za* $x = 30$.
Među brojevima od 1 do 30 prosti su: $2, 3, 5, 7, 11, 13, 17, 19, 23$ *i* 29.
Njih je ukupno 10 *pa je* $\pi(30) = 10$.

Na sljedećim grafovima možemo vidjeti kako se ponaša funkcija $\pi(x)$ za $x \leq 30$ i $x \leq 100$:



Slika 2.1: Graf funkcije $\pi(x)$ za $x \leq 30$



Slika 2.2: Graf funkcije $\pi(x)$ za $x \leq 100$

Iako se prosti brojevi među prirodnima pojavljuju nasumično i naizgled bez pravila, iz prethodnih grafova možemo uočiti da što je x veći, to graf ima pravilniji oblik. Matematičari su stoljećima pokušavali pronaći prikladnu aproksimiraciju

funkcije $\pi(x)$, a prvu značajnu pretpostavku objavio je **Adrien-Marie Legendre** (1752. – 1833.) u svojoj knjizi *Essai sur la thèorie des nombres* 1808. godine ([5]). Na temelju tada poznatih vrijednosti funkcije $\pi(x), x \leq 400\,000$, tvrdio je sljedeće:

$$\pi(x) \sim \frac{x}{\ln x - 1.08366}, \text{ kada } x \to \infty. \tag{2.15}$$

Carl Friedrich Gauss (1777. – 1855.) također je proučavao tablicu prostih brojeva i svoju procjenu za funkciju $\pi(x)$ odredio je 1791. godine, sa samo 14 godina, no prvi put spominje ju tek 1849. godine u svojemu pismu **Johannu Franzu Enckeu** (1844. – 1865.). Njegova je procjena objavljena tek 1863. godine i izgledala je ovako:

$$\pi(x) \sim \mathrm{Li}(x) = \int_2^x \frac{dt}{\ln t}, \text{ kada } x \to \infty. \tag{2.16}$$

Prvi matematičar koji je napravio veliki korak prema dokazu teorema, danas poznatog kao teorem o prostim brojevima, bio je **Pafnuti Čebišev** (1821. – 1894.). On je 1850. godine pokazao da postoje konstante $a \leq 1 \leq b$ takve da je

$$a\frac{x}{\ln(x)} \leq \pi(x) \leq b\frac{x}{\ln(x)}$$

i da, ako postoji $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x}$, on mora biti jednak 1 ([18]).

Najznačajniji doprinos, koji je doveo do samoga dokaza teorema o prostim brojevima, dao je njemački matematičar **Bernhardt Riemann** (1826. – 1866.). On je u svojemu djelu *Über die Anzhal der Primzhalen unter eine gegebenen Grösse* iz 1859. godine zeta funkciju predstavio kao funkciju kompleksne varijable:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \forall s \in \mathbb{C}, Re(s) > 1,$$

za razliku od Eulera koji ju je razmatrao samo kao funkciju realne varijable. Nadalje, pokazao je da se ona može analitički proširiti na sve kompleksne brojeve, osim $s = 1$, te da je $\zeta(s) = 0$ za $s = -2n, n \in \mathbb{N}$, i takve nultočke nazivaju se trivijalne nultočke Riemannove zeta funkcije. Matematičarima su zanimljive upravo one netrivijalne, a one leže unutar tzv. *kritične pruge* $0 < Re(s) < 1$ ([8]). Riemann je tvrdio sljedeće:

Slutnja 1 (Riemannova slutnja, vidi [8])**.** *Sve netrivijalne nultočke Riemannove zeta funkcije ζ leže na pravcu $Re(s) = \frac{1}{2}, s \in \mathbb{C}, s \neq 1$.*

Napokon, 1896. godine, neovisno jedan o drugome, **Jacques Salomon Hadamard** (1865. – 1963.) i **Charles Jean de la Vallèe Poussin** (1866. – 1962.) dokazali su sljedeći teorem:

Teorem 13 (Teorem o prostim brojevima, vidi [24])**.** *Vrijedi sljedeće:*

$$\pi(x) \sim \frac{x}{\ln(x)}, \text{ kada } x \to \infty. \tag{2.17}$$

U dokazu su koristili rezultate iz kompleksne analize te svojstva Riemannove zeta funkcije. Pokazali su da ne postoje netrivijalne nultočke za $Re(s) = 1$, tj. da je $\zeta(1+it) \neq 0$, i dali su sljedeću ocjenu greške za aproksimaciju (2.17):

$$\pi(x) = \mathrm{Li}(x) + O\left(xe^{-a\sqrt{\ln x}}\right), {}^{2} a \in \mathbb{R}^{+}.$$

Riemannova slutnja daje oštriju ocjenu greške:

Slutnja 2 (Ekvivalent Riemannove slutnje, vidi [8])**.** *Vrijedi:*

$$\pi(x) = \mathrm{Li}(x) + O\left(\sqrt{x}\ln x\right),$$

tj.

$$\exists c > 0 : \ |\pi(x) - \mathrm{Li}(x)| \leq c\sqrt{x}\ln x.$$

Riemannova je slutnja jedan od 7 milenijskih problema. Za sada je provjereno prvih 10^{13} netrivijalnih rješenja jednadžbe $\zeta(s) = 0$ i sva leže na pravcu $Re(s) = \frac{1}{2}$, tj. za sada nije pronađena niti jedna netrivijalna nultočka koja bi opovrgnula ovu slutnju. Nagrada za njezino rješenje iznosi 1 000 000$ (Clay Mathematics Institute - Riemann hypothesis).

Kasnije su, neovisno jedan o drugome, matematičari **Atle Selberg** (1917. – 2007.) i **Paul Erdös** (1913. – 1996.) dali elementarni dokaz Teorema 13. Važno je naglasiti da se izraz *elementarni* ne odnosi na jednostavniji dokaz, nego na dokaz bez korištenja kompleksne analize i Riemannove zeta funkcije. Upravo suprotno, ovaj je dokaz puno složeniji od prvobitnoga (vidi [16] i [11]).

Pokažimo da su aproksimacije (2.15) i (2.16) ekvivalentne aproksimaciji (2.17) iz Teorema 13. Koristit ćemo L'Hospitalovo pravilo i pravila za deriviranje umnoška i količnika. Prema Teoremu 13 je $\pi(x) \sim \frac{x}{\ln x}$ pa je

$$\pi'(x) \approx \left(\frac{x}{\ln x}\right)' = \frac{x'\ln x - x(\ln x)'}{\ln^2 x} = \frac{1}{\ln x} - \frac{1}{\ln^2 x}.$$

Pokažimo da je:

- $\pi(x) \sim \frac{x}{\ln x + B}$:

$$\begin{aligned}
\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x+B}} &= \lim_{x\to\infty} \frac{\pi(x)(\ln x + B)}{x} \\
&= \lim_{x\to\infty} \frac{\pi'(x)(\ln x + B) + \pi(x)(\ln(x) + B)'}{x'} \\
&= \lim_{x\to\infty} \left[\left(\frac{1}{\ln x} - \frac{1}{\ln^2 x}\right)(\ln x + B) + \frac{\pi(x)}{x}\right] \\
&= \lim_{x\to\infty} \left[1 + \frac{B}{\ln x} - \frac{1}{\ln x} - \frac{B}{\ln^2 x} + \frac{1}{\ln x}\right] \\
&= 1.
\end{aligned}$$

[2] Neka su $f(n)$ i $g(n)$ dvije funkcije i $n > 0$. Kažemo da je f veliko-O od g, i pišemo $f(n) \in O(g(n))$ ako postoje pozitivne konstante c i C takve da je $f(n) \leq cg(n)$, $\forall n \geq C$.

Kako ovo vrijedi za bilo koju konstantu B, onda vrijedi i za $B = -1.08366$ koja je u aproksimaciji (2.15).

- $\pi(x) \sim \int_2^x \frac{dt}{\ln t}$:

$$\lim_{x\to\infty} \frac{\pi(x)}{\int_2^x \frac{dt}{\ln t}} = \lim_{x\to\infty} \frac{\pi'(x)}{\left(\int_2^x \frac{dt}{\ln t}\right)'} = \lim_{x\to\infty} \frac{\frac{1}{\ln x} - \frac{1}{\ln^2 x}}{\frac{1}{\ln x}} = \lim_{x\to\infty} \left(1 - \frac{1}{\ln x}\right) = 1.$$

Pokazalo se da je upravo (2.16) najbolja aproksimacija za $\pi(x)$, a to možemo vidjeti i u sljedećoj tablici jer će, kako x raste, upravo ona biti najbliža stvarnoj vrijednosti funkcije $\pi(x)$:

x	$\pi(x)$	$\frac{x}{\ln(x)}$	$\frac{x}{\ln(x)-1.08366}$	$\int_2^x \frac{dt}{\ln(t)}$
10	4	4	8	5
10^2	25	22	28	29
10^3	168	145	172	177
10^4	1229	1086	1231	1245
10^5	9592	8686	9588	9629
10^6	78 498	72 382	78 543	78 627
10^7	664 579	620 421	665 140	664 917
10^8	5 761 455	5 428 681	5 768 004	5 762 208
10^9	50 847 534	48 254 942	50 917 519	50 849 234
10^{10}	455 052 511	434 294 482	455 743 004	455 055 614
10^{11}	4 118 054 813	3 948 131 654	4 124 599 869	4 118 066 400

Tablica 2.4: Tablica vrijednosti funkcije $\pi(x)$ i njezinih aproksimacija

Pogledajmo posljedice Teorema 13 ([3]):

1: Teorem 13 implicira da se za aproksimaciju funkcije $\pi(x)$ može uzeti funkcija $\frac{x}{\ln x - a}$, pri čemu je a bilo koja konstanta. U Teoremu 13 je $a = 0$, a u Legendreovoj je aproksimaciji (2.15) $a = 1.08366$, no ispostavilo se da je $a = 1$ bolji odabir.

2: Ukoliko s p_n označimo n-ti prost broj, Teorem 13 ekvivalentan je sljedećem:

$$p_n \sim n \ln n, \text{ kada } n \to \infty.$$

Dokaz. Ako je p_n n-ti prost broj i $\pi(n) = \sum_{p \le n} 1$, onda je $\pi(p_n) = n$. Iz Teorema 13 slijedi da je

$$n \sim \frac{p_n}{\ln p_n}, \text{ kada } n \to \infty. \tag{2.18}$$

Pokažimo da je $\ln p_n \sim \ln n$, kada $n \to \infty$.
Iz (2.18) je

$$\ln n \sim \ln\left(\frac{p_n}{\ln p_n}\right) = \ln p_n - \ln\ln p_n, \text{ kada } n \to \infty. \tag{2.19}$$

Ako stavimo da je $m = p_n$ i iskoristimo da $m \to \infty$ kada $n \to \infty$, onda imamo da je

$$\lim_{n\to\infty} \frac{\ln n}{\ln p_n} = \lim_{m\to\infty} \frac{\ln m - \ln\ln m}{\ln m} = \lim_{m\to\infty}\left[1 - \frac{\ln\ln m}{\ln m}\right] = \lim_{m\to\infty}\left[1 - \frac{\frac{1}{\ln m}\cdot\frac{1}{m}}{\frac{1}{m}}\right]$$
$$= 1,$$

pri čemu prva jednakost slijedi iz (2.19), a predzadnja zbog L'Hospitalovog pravila. Sada smo pokazali da je $\ln n \sim \ln p_n$, a iz (2.18) je

$$p_n \sim n\ln p_n \sim n\ln n, \text{ kada } n \to \infty.$$

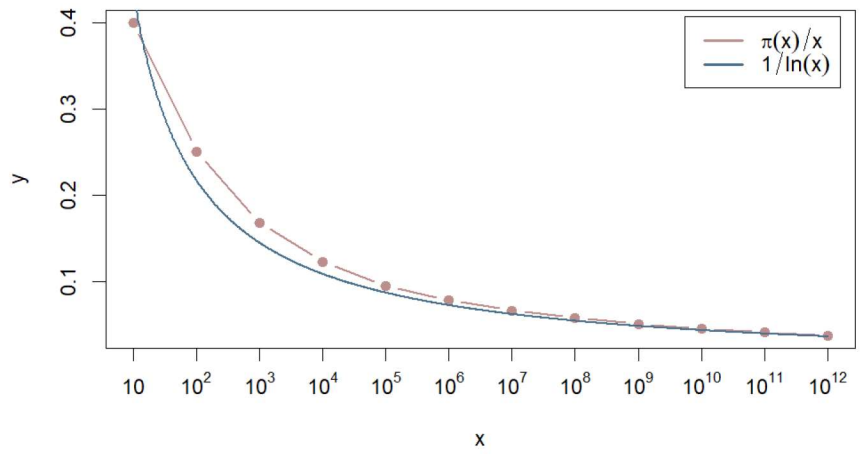
□

3: Frekvencija prostih brojeva manjih ili jednakih od x približno je jednaka $\frac{1}{\ln x}$, tj.

$$\frac{\pi(x)}{x} \sim \frac{1}{\ln x}, \text{ kada } x \to \infty.$$

Ekvivalentno je i reći da će među brojevima od 1 do x njih približno $\frac{1}{\ln x}$ biti prosto.

Iz sljedećega grafa možemo uočiti da kako x raste, frekvencija prostih brojeva smanjuje se, tj. prosti brojevi prorjeđuju se za sve veći x:



Slika 2.3: Graf funkcije $\frac{\pi(x)}{x}$ i njene aproksimacije $\frac{1}{\ln x}$

3 | Testovi prostosti

Testove prostosti koristimo kada želimo provjeriti je li neki broj prost ili nije. Oni su vrlo važan dio mnogih kriptosustava, a samo jedan među njima je i poznati RSA kriptosustav čija se sigurnost temelji na teškoći faktorizacije velikih složenih brojeva. Htjeli bismo da test bude:

1. **OPĆI** - želimo da test bude primjenjiv na svim brojevima, a ne samo onima posebnoga oblika.
2. **DETERMINISTIČAN** - test bi uvijek trebao točno odrediti je li broj prost ili ne. S druge su strane vjerojatnosni testovi kod kojih postoji mogućnost da složen broj pogrešno proglase prostim, no uz nekoliko ponavljanja testa ta se greška može učiniti dovoljno malom.
3. **BEZUVJETAN** - poželjno je da se test ne oslanja na nedokazane tvrdnje (npr. Riemannovu slutnju).
4. **POLINOMIJALNOGA VREMENA IZVOĐENJA** - vremenska se složenost algoritma treba moći opisati funkcijom polinoma f čiji će argument biti veličina ulaza n. Za testiranje prostosti, veličina ulaza n mjeri se brojem bitova potrebnih za prikaz broja n i iznosi približno $\log_2(n)$. Dakle, polinomjalno vrijeme algoritma imat će složenost $f(\log_2(n))$, pri čemu je f funkcija polinoma. Sve do 2002. godine nije bilo poznato je li problem određivanja prostosti polinomijalnoga vremena izvođenja, no ispostavilo se da je.

U ovome poglavlju testovi su podijeljeni na deterministčke i vjerojatnosne ([22]), dok se na samome kraju spominje dokazivanje prostosti eliptičkim krivuljama ([10]).

3.1 Deterministički testovi

Kao što je u uvodnom dijelu ovoga poglavlja spomenuto, deterministički testovi uvijek će točno odrediti je li neki broj prost ili ne. Sporiji su od vjerojatnosnih testova, no preferiraju se u slučajevima kada ni mala vjerojatnost greške u određivanju prostosti nije dopuštena.

Prisjetimo se definicije koja će nam biti potrebna za dokaz sljedećega teorema:

Definicija 20. *Neka je p prost broj i $a \in \mathbb{N}, a < p$. Multiplikativni inverz od a modulo p je broj $b \in \mathbb{N}$ za koji vrijedi $ab \equiv 1 \pmod{p}$.*

Sljedeća dva teorema zajedno nam daju karakterizaciju prostih brojeva:

Teorem 14 (Wilsonov teorem, vidi [14]). *Ako je p prost broj, onda je* $(p-1)! \equiv -1 \pmod{p}$.

Dokaz. Neka je p prost broj. Za svaki od brojeva $1, 2, \ldots, p-1$ postoji multiplikativni inverz modulo p. To znači da je svaki od faktora u $(p-1)! = 1 \cdot 2 \cdots (p-1)$ u produktu sa svojim inverzom kongruentan 1 modulo p, osim faktora koji su sami sebi inverzni. Pogledajmo koji su to faktori. Neka je $x \in \{1, 2, \ldots, p-1\}$ takav da je $x^2 \equiv 1 \pmod{p}$. Tada $p | x^2 - 1 = (x-1)(x+1)$. S obzirom na to da je p prost broj i $1 \leq x \leq p-1$, vrijedi da je $x - 1 = 0$ ili $x + 1 = p$. To znači da su 1 i $p-1$ jedini faktori u $(p-1)!$ koji su sami sebi inverzni te slijedi:

$$(p-1)! \equiv 1 \cdot (p-1) \pmod{p}, \text{ tj.}$$
$$(p-1)! \equiv -1 \pmod{p}.$$

□

Za otkriće gornjega teorema najvjerojatnije je zaslužan **Ibn al–Haytham** (965. – 1040.), a **Edward Waring** (1736. – 1798.) objavio ga je bez dokaza 1770. godine pripisujući zasluge otkrića svojem učeniku **Johnu Wilsonu** (1741 – 1793.). Godinu dana kasnije, dokazao ga je **Joseph – Louis Lagrange** (1736. – 1813.) te je pokazao da vrijedi i obrat teorema:

Teorem 15 (Lagrangeov teorem, vidi [14]). *Ako $n \in \mathbb{N}$ zadovoljava kongruenciju $(n-1)! \equiv -1 \pmod{n}$, onda je n prost broj.*

Dokaz. Neka je $n \in \mathbb{N}$ takav da vrijedi kongruencija $(n-1)! \equiv -1 \pmod{n}$. Dokaz se provodi kontradikcijom pa ćemo pretpostaviti da je n složen i da je $m < n$ djelitelj od n. Iz $m | n$ slijedi da je $(n-1)! \equiv -1 \pmod{m}$. S druge strane, iz $m < n$ znamo da je m jednak jednom od faktora u $(n-1)! = 1 \cdot 2 \cdots (n-1)$ pa je $(n-1)! = 0 \pmod{m}$. Dobivamo da je $-1 \equiv 0 \pmod{m}$ iz čega je jasno da je $m = 1$. Zaključujemo da n nema pozitivnih djelitelja različitih od 1 i n pa je on prost. □

Test temeljen na prethodna dva teorema nije praktičan za upotrebu jer faktorijeli vrlo brzo rastu. Upravo se zbog toga prednost daje nekim drugim testovima koje ćemo spomenuti u nastavku ovoga poglavlja.

3.1.1 Probno dijeljenje

Probno dijeljenje najjednostavniji je i najstariji test za određivanje prostosti, odnosno složenosti nekoga broja $n \in \mathbb{N}, n > 1$. Usko je povezan s Eratostenovim sitom te slijedi iz Propozicije 7 čiji obrat po kontrapoziciji daje ekvivalentnu tvrdnju:
Ako ne postoji djelitelj $d \in \mathbb{N}$ od n takav da je $1 < d \leq \lfloor \sqrt{n} \rfloor$, onda je n prost broj.

Također, obrat po kontrapoziciji Korolara 5 daje nam sljedeće:
Ukoliko ne postoji prosti djelitelj p nekoga broja n za kojega vrijedi $p \leq \lfloor \sqrt{n} \rfloor$,

onda će n biti prost broj.

Algoritam probnoga dijeljenja izgleda ovako ([22]):

Algoritam 1 Algoritam probnoga dijeljenja

input: $n \geq 2$
for $i = 2$ to $\lfloor \sqrt{n} \rfloor$ **do**
  if $i | n$ **then**
    return composite
return prime

3.1.2 AKS test

AKS test prvi je test prostosti koji ima sve četiri poželjne karakteristike - opći je, deterministčan, bezuvjetan i polinomijalnoga vremena izvođenja. Predstavili su ga 2002. godine računalni znanstvenici **Manindra Agrawal**, **Neeraj Kajal** i **Nitin Saxena** u svojemu radu *Pimes is in P* (vidi [2]). Naknadno su napravljena poboljšanja testa vezana uz vrijeme izvođenja algoritma te je ponovno objavljen 2004. godine.

AKS test temelji se na generalizaciji malog Fermatovog teorema (Teorem 11) na polinome:

Teorem 16 (vidi [22]). *Neka je $n \geq 2$ i $a < n$ takav da $(a, n) = 1$. Tada je n prost ako i samo ako vrijedi:*

$$(X + a)^n \equiv X^n + a \pmod{n}, \tag{3.1}$$

pri čemu je $X \in \mathbb{Z}_n[X]$, a $\mathbb{Z}_n[X]$ je prsten polinoma.

Dokaz. Neka je $n \geq 2$ i $a < n$ takav da $(a, n) = 1$. Iz binomnog teorema je

$$(X + a)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} X^i. \tag{3.2}$$

Koeficijent uz X^i u razvoju polinoma $(X + a)^n$ jednak je $\binom{n}{i} a^{n-i}$.

$\Longrightarrow$ Pretpostavimo da je n prost. Tada za $0 < i < n$ vrijedi da je $\binom{n}{i} = \frac{n!}{i!(n-i)!} \equiv 0 \pmod{n}$, jer n dijeli brojnik, ali ne i nazivnik $(i, n - i < n)$.
Za $i = 0$, dobivamo izraz a^n jer je $X^0 = 1$ i $\binom{n}{0} = 1$.
Za $i = n$, dobivamo izraz X^n jer je $a^{n-n} = 1$ i $\binom{n}{n} = 1$.
Iz toga slijedi:

$$(X + a)^n \equiv a^n + 0 + 0 + \cdots + 0 + X^n \pmod{n}.$$

Prema Teoremu 11 je $a^n \equiv a \pmod{n}$ pa je

$$(X + a)^n \equiv X^n + a \pmod{n}.$$

$\Longleftarrow$ Za dokaz ovoga smjera koristimo obrat po kontrapoziciji. Pretpostavimo da je n složen. Neka je q prost broj koji dijeli n i neka je k potencija od q u faktorizaciji broja n. Uočimo da je $1 < q < n$ i $q^k | n$, ali $q^{k+1} \nmid n$. Pogledajmo koeficijent uz X^q u (3.2):

$$\binom{n}{q} a^{n-q} = \frac{n!}{q!(n-q)!} a^{n-q} = \frac{n(n-1)\cdots(n-q+1)}{q!} a^{n-q}.$$

Uočimo da $q^k | n$, ali svi ostali faktori u brojniku relativno su prosti s q. Slijedi da je brojnik djeljiv s q^k, ali ne i s q^{k+1}. Djelitelj od q u nazivniku pokrati se s nekim od q-ova u brojniku te tada cijeli razlomak nije djeljiv s q^k. Kako je $(a, n) = 1$, onda je i $(q^k, a^{n-q}) = 1$. S obzirom na to da q^k ne dijeli $\binom{n}{q} a^{n-q}$, onda ga ni n ne dijeli jer $q^k | n$. Stoga, koeficijent od X^q je $\not\equiv 0 \pmod{n}$. Kako je $1 < q < n$, slijedi da je

$$(X + a)^n \not\equiv X^n + a \pmod{n}.$$

□

Računanje koeficijenata u razvoju polinoma $(X + a)^n$ činilo je ovaj test poprilično sporim za velike n i zbog toga je napravljeno ranije spomenuto poboljšanje testa. Naime, pomak je napravljen u evaluaciji polinoma s obje strane kongruencije (3.1) modulo neki polinom $X^r - 1$ te provjeri za nekoliko različitih odabira za a. Dakle, testira se kongruencija:

$$(X + a)^n \equiv X^n + a \pmod{n, X^r - 1}. \tag{3.3}$$

Prvobitna kongruencija (3.2) gledana je u prstenu polinoma $\mathbb{Z}_n[X]$, a prethodna se kongruencija (3.3) promatra u kvocijentnom prstenu polinoma $\mathbb{Z}_n[X]/(X^r - 1)$. Dakle, elemente kvocijentnog prstena polinoma gledamo kao elemente prstena polinoma modulo $X^r - 1$. Zbog toga ćemo najprije koeficijente s obje strane kongruencije (3.3) reducirati modulo n, a potome ćemo reducirati stupnjeve polinoma modulo $X^r - 1$ pomoću relacije $X^r \equiv 1 \pmod{X^r - 1}$. Na kraju provjeravamo jesu li one međusobno kongruentne modulo $n, X^r - 1$ ([22]).

Algoritam AKS testa izgleda ovako ([22]):

Algoritam 2 AKS algoritam

input: $n \geq 2$
if $n = b^k$ for $b, k > 1$ **then**
  return composite
find the smallest r such that $ord_r(n) > \log_2^2 n$
if $1 < (a, n) < n$ for some $a \leq r$ **then**
  return composite
if $n \leq r$ **then**
  return prime
for $a = 1$ to $\lfloor \sqrt{\varphi(r)} \log_2 n \rfloor$ **do**
  if $(X + a)^n \not\equiv X^n + a \pmod{n, X^r - 1}$ **then**
    return composite
return prime

Funkcija φ u prethodnom algoritmu je Eulerova funkcija.

3.1.3 Lucas – Lehmerov test

Lucas – Lehmerov test deterministički je test kojim se određuje je li Mersenneov broj $M_n = 2^n - 1$ prost ili složen. Razvio ga je 1878. godine francuski matematičar **François Èdouard Anatole Lucas** (1842. – 1891.), a 1930. godine dokazao ga je američki matematičar **Derrich Henry Lehmer** (1905. – 1991.). Test se temelji na sljedećem teoremu:

Teorem 17 (Lucas – Lehmerov teorem, vidi [14]). *Definiramo niz prirodnih brojeva* (s_n) *na sljedeći način:*

$$s_1 = 4, \quad s_{n+1} = s_n^2 - 2.$$

Neka je p *neparan prost broj. Mersenneov broj* M_p *je prost ako i samo ako* $M_p | s_{p-1}$.

Primjer 7. *Koristeći Lucas – Lehmerov teorem pokažimo da je* M_7 *prost broj.*

Rješenje. Najprije izračunamo $M_7 = 2^7 - 1 = 127$, a potom $s_i = s_{i-1}^2 - 2$ za $2 \leq i \leq 6$ i provjeravamo vrijedi li da $M_7 | s_6$, tj. je li $s_6 \equiv 0 \pmod{127}$.

$$\begin{aligned}
s_1 &= 4, \\
s_2 &= (4^2 - 2) \equiv 14 \pmod{127}, \\
s_3 &= (14^2 - 2) \equiv 67 \pmod{127}, \\
s_4 &= (67^2 - 2) \equiv 42 \pmod{127}, \\
s_5 &= (42^2 - 2) \equiv 111 \pmod{127}, \\
s_6 &= (111^2 - 2) \equiv 0 \pmod{127}.
\end{aligned}$$

Pokazali smo da je M_7 prost broj.

Algoritam Lucas – Lehmerovog test izgleda ovako ([9]):

Algoritam 3 Lucas – Lehmerov algoritam

input: odd prime number n
calculate $M_n = 2^n - 1$
$s_1 \leftarrow 4$
for $i = 2$ to $n - 1$ **do**
    $s_i \leftarrow (s_{i-1}^2 - 2) \pmod{M_n}$
if $s_{n-1} = 0$ **then**
    return prime
return composite

3.1.4 Pepinov test

Pepinov test deterministički je test kojim se provjerava prostost Fermatovih brojeva $F_n = 2^{2^n} + 1$. Francuski matematičar **Jean François Thèophile Pèpin** (1826. – 1904.) pokazao je 1877. godine da vrijedi sljedeći teorem:

Teorem 18 (Pepinov teorem, vidi [13])**.** *Fermatov broj $F_n = 2^{2^n} + 1$ je prost ako i samo ako je $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.*

Primjer 8. *Koristeći Pepinov teorem pokažimo da je F_2 prost broj.*

Rješenje. Vrijedi sljedeće:

$$F_2 = 2^{2^2} + 1 = 17,$$
$$3^{\frac{17-1}{2}} = 3^8 = 6561 \equiv 16 \equiv -1 \pmod{17}.$$

Pokazali smo da je F_2 prost broj.

Algoritam Pepinovog testa izgleda ovako:

Algoritam 4 Algoritam Pepinovog testa

input: $n \in \mathbb{N}$
calculate $F_n = 2^{2^n} + 1$
if $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$ **then**
    return prime
return composite

3.2 Vjerojatnosni testovi

Vjerojatnosni testovi, za razliku od deterministčkih, ne mogu utvrditi je li broj koji testiramo sigurno prost, ali to mogu učiniti s velikom vjerojatnošću. S druge strane, ukoliko neki broj proglase složenim, sigurni smo da je to stvarno tako. Za provođenje ovakvih testova potrebne su nam dvije veličine:

- broj n čiju prostost želimo ispitati;

- slučajno odabrani broj $a \in \{2, \ldots, n-1\}$.

Test će vratiti jedan od rezultata - *složen* ili *vjerojatno prost*. Ukoliko test proglasi neki broj složenim, broj a naziva se **svjedokom složenosti** broja n. Glavna je ideja testirati n za nekoliko vrijednosti a te ukoliko bilo koji od testova pokaže da je n složen, gotovi smo s testiranjem. Ukoliko svi testovi pokažu da je n vjerojatno prost, možemo samo biti sve više uvjereni da će on stvarno biti prost ([22]). U sljedećim potpoglavljima razmotrit ćemo nekoliko vjerojatnosnih testova.

3.2.1 Fermatov test

Fermatov je test vjerojatnosni test temeljen na Teoremu 11.

Obrat po kontrapoziciji daje ekvivalentnu tvrdnju:
Ako postoji $a > 1$, takav da je $(a, n) = 1$ i $a^{n-1} \not\equiv 1 \pmod{n}$, onda je n složen.

Obrat malog Fermatovog teorema ne vrijedi, tj. ukoliko je $a^{n-1} \equiv 1 \pmod{n}$ za svaki $a > 1$ koji je relativno prost s n, to ne znači da će n biti prost.

U nastavku ovoga potpoglavlja reći ćemo nešto više o složenim brojevima koji, baš kao i prosti brojevi, zadovoljavaju kongruenciju malog Fermatovog teorema i na taj način nadmudre ovaj test jer ih on proglasi vjerojatno prostima.

Definicija 21. *Za složeni broj $n \in \mathbb{N}$ kažemo da je pseudoprost u bazi a ako je*

$$a^{n-1} \equiv 1 \pmod{n},$$

pri čemu je $(a, n) = 1$ i $a > 1$.

Primjer 9. *Pokažimo da je broj 25 pseudoprost u bazi 7, ali da nije pseudoprost u bazi 2.*

Rješenje. Primijetimo da vrijedi da je $(25, 7) = 1$ i $(25, 2) = 1$.
Prvo trebamo pokazati da je $7^{25-1} = 7^{24} \equiv 1 \pmod{25}$.

$$\begin{aligned} 7^2 &= 49 \equiv 24 \equiv -1 \pmod{25}, \\ 7^4 &= (7^2)^2 \equiv (-1)^2 \equiv 1 \pmod{25}, \\ 7^{24} &= (7^4)^6 \equiv 1^6 \equiv 1 \pmod{25}. \end{aligned}$$

Preostaje pokazati da broj 25 nije pseudoprost u bazi 2, tj. da $2^{24} \not\equiv 1 \pmod{25}$.

$$\begin{aligned} 2^2 &\equiv 4 \pmod{25}, \\ 2^4 &\equiv 16 \pmod{25}, \\ 2^8 &= 256 \equiv 6 \pmod{25}, \\ 2^{24} &= 2^8 \cdot 2^{16} \equiv 6 \cdot 11 = 66 \equiv 16 \not\equiv 1 \pmod{25}. \end{aligned}$$

Definicija 22. *Složeni broj $n \in \mathbb{N}$ naziva se Carmichaelov broj ako za svaku bazu $a \in \{2, \ldots, n-1\}$ takvu da je $(a, n) = 1$ vrijedi:*

$$a^{n-1} \equiv 1 \pmod{n}.$$

Uočavamo da je složeni broj n Carmichaelov ako i samo ako je pseudoprost za svaku bazu a. Također, iz prethodnoga primjera i definicije zaključujemo da je svaki Carmichaelov broj pseudoprost, ali nije svaki pseudoprost broj Carmichaelov.

Carmichaelovi brojevi dobili su ime po američkom matematičaru **Robertu Danielu Carmichaelu** (1879. – 1967.) koji je tvrdio da ih ima beskonačno mnogo, a 1994. godine to je i dokazano ([1]). Oni su svi neparni ([14]) i produkt su najmanje tri različita prosta broja ([7]).

Carmichaelovi brojevi rijetki su i to potvrđuje činjenica da ih je samo 2163 među prvih 25 milijardi brojeva, a najmanji je $561 = 3 \cdot 11 \cdot 17$ ([17]).

Fermatov test Carmichaelove brojeve za svaki odabir baze a svrstava među vjerojatno proste brojeve. Broj a tada nazivamo **Fermatov lažov**.

Kada Fermatovim testom za neki broj n želimo provjeriti je li prost ili složen, k puta nasumično odabiremo bazu $a \in \{2, \ldots, n-1\}$ i provjeravamo vrijedi li kongruencija $a^{n-1} \equiv 1 \pmod{n}$. U slučaju da za bilo koji k kongruencija ne vrijedi, znamo da je broj n sigurno složen. Ukoliko vrijedi u svakoj, n je vjerojatno prost.

Algoritam Fermatovog testa izgleda ovako ([22]):

Algoritam 5 Algoritam Fermatovog testa

input: $n > 3, k \in \mathbb{N}$
for $i = 1$ to k **do**
  choose random $a \in \{2, \ldots, n-1\}$
  if $a^{n-1} \not\equiv 1 \pmod{n}$ **then**
    return composite
return probably prime

Broj k u algoritmu predstavlja broj nezavisnih iteracija. U jednoj iteraciji ovoga testa vjerojatnost da se složen broj proglasi prostim manja je od $\frac{1}{2}$. Što veći k odaberemo, greška će biti manja, tj. iznosit će manje od $\left(\frac{1}{2}\right)^k$.

3.2.2 Miller – Rabinov test

Miller – Rabinov test poboljšava nedostatke Fermatovog testa jer se temelji na jakoj pseudoprostosti koju ćemo u nastavku definirati. Računalni znanstvenik **Gary Lee Miller** (1944. – 2024.) zaslužan je za prvobitnu verziju ovoga testa predstavljenu 1976. godine, a ona je bila deterministička i temeljena na proširenoj Riemannovoj slutnji. Kasnije je matematičar i računalni znanstvenik **Michael Oser Rabin** predložio vjerojatnosnu verziju testa koja je izostavila korištenje

nedokazane Riemannove slutnje.

Test se temelji na sljedećoj propoziciji:

Propozicija 24 (vidi [22]). *Neka je p neparan prost broj i zapišimo ga na sljedeći način:*

$$p - 1 = 2^k q, \text{ gdje je } q \text{ neparan.}$$

Neka je a bilo koji broj relativno prost s p. Tada je jedan od sljedećih uvjeta istinit:

i) $a^q \equiv 1 \pmod{p}$.

ii) Jedan je od $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}$ *kongruentan* $-1 \pmod{p}$.

Dokaz. Prema Teoremu 11 vrijedi da je $a^{p-1} \equiv 1 \pmod{p}$. Pogledamo li niz brojeva

$$a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}, a^{2^k q},$$

primjećujemo da zbog $p - 1 = 2^k q$ i Teorema 11, za posljednji član vrijedi sljedeće:

$$a^{2^k q} = a^{p-1} \equiv 1 \pmod{p}.$$

Kako je svaki broj niza (osim prvoga), kvadrat prethodnoga broja u nizu, jedno od sljedećega vrijedi:

i) prvi broj u nizu, a^q, kongruentan je 1 modulo p

ii) neki od brojeva u nizu nije kongruentan 1 modulo p, ali to postane kada se kvadrira. Jedini broj koji zadovoljava oba spomenuta uvjeta

$$b \not\equiv 1 \pmod{p} \quad \text{i} \quad b^2 \equiv 1 \pmod{p}$$

je broj -1 pa je jedan od članova u nizu kongruentan -1 modulo p.

□

Za složen broj koji zadovoljava prethodnu propoziciju kažemo da je **jak pseudoprosti broj u bazi** a.

Kada Miller – Rabinovim testom za neki neparan broj n želimo provjeriti je li prost ili složen, prvo ćemo nasumično odabrati bazu $a \in \{2, \ldots, n-2\}$ koja je relativno prosta s n. Zatim ćemo n zapisati u obliku $n - 1 = 2^k m$. Nakon toga računamo $b_0 \equiv a^m \pmod{n}$ i provjeravamo je li kongruentan $\pm 1 \pmod{n}$. Ukoliko je, broj n proglašavamo vjerojatno prostim. Ukoliko nije, za $i = 1, \ldots, k-1$ provjeravamo je li neki od brojeva $b_i = b_{i-1}^2$ kongruentan -1 modulo n jer ako je, n će biti vjerojatno prost. U slučaju da za svaku iteraciju vrijedi da je $b_i \not\equiv -1 \pmod{n}$, broj n bit će proglašen složenim, a baza a bit će svjedok složenosti od n.

Algoritam Miller – Rabinovog testa izgleda ovako ([9]):

Algoritam 6 Miller – Rabinov algoritam

input: odd number $n > 3$
choose random $a \in \{2, \ldots, n-2\}$
if $(a, n) > 1$ **then**
    return composite
write n as $n - 1 = 2^k m$, where m is odd
$b_0 \leftarrow a^m \pmod{n}$
if $b_0 \equiv \pm 1 \pmod{n}$ **then**
    return probably prime
for $i = 1$ to $k - 1$ **do**
    $b_i \leftarrow b_{i-1}^2 \pmod{n}$
    if $b_i \equiv -1 \pmod{n}$ **then**
        return probably prime
return composite

Kod Miller – Rabinovog testa vjerojatnost da se složen broj pogrešno ocijeni prostim u jednoj iteraciji manja je od $\frac{1}{4}$. Za k nezavisnih iteracija ta greška iznosi manje od $\left(\frac{1}{4}\right)^k$. Odmah uočavamo da je manja nego kod Fermatovog testa.

3.2.3 Solovay – Strassenov test

Solovay – Strassenov test vjerojatnosni je test kojega su 1977. godine razvili američki matematičar **Robert Martin Solovay** i njemački matematičar **Volker Strassen**, a temelji se na kvadratnim ostatcima (Definicija 15), Jacobijevom i Legendreovom simbolu (Definicija 16) te Eulerovom kriteriju (Teorem 12).

Jacobijev simbol generalizacija je Legendreovog simbola. Neka je $P \in \mathbb{N}$ i zapišimo ga u obliku $P = p_1 p_2 \cdots p_n$, gdje su p_i neparni prosti brojevi. Jacobijev simbol definiran je na sljedeći način:

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_n}\right) = \prod_{i=1}^{n}\left(\frac{a}{p_i}\right).$$

Ako je broj P prost, onda se Jacobijev i Legendreov simbol podudaraju. Nedostatak Jacobijevog simbola proizlazi iz činjenice da $\left(\frac{a}{P}\right) = 1$ ne znači da je a kvadratni ostatak modulo P. Vrijedi:

$$a \text{ je kvadratni ostatak modulo } P \iff$$
$$a \text{ je kvadratni ostatak modulo } p_i, \forall 1 \leq i \leq n.$$

Teorem 19 (Solovay – Strassenov teorem, vidi [23]). *Neka je $n \in \mathbb{N}, n > 1$ i nasumično odaberimo brojeve $a_1, a_2, \ldots, a_k \in \mathbb{N}$ takve da je $0 < a_i < n$ i $(a_i, n) = 1, \forall i \in \{1, \ldots, k\}$. Računamo:*

$$a_i^{\frac{n-1}{2}} \equiv \left(\frac{a_i}{n}\right) \pmod{n}, \quad i = 1, 2, \ldots, k.$$

Ako za neki indeks i ta kongruencija ne vrijedi, broj n je složen.

Prethodni se teorem često naziva i *Eulerov test pseudoprostosti*.
Slučajno odabrana baza a za koju složeni broj n nadmudri Eulerov test zove se **Eulerov lažov**, a takav broj n naziva se **Eulerov pseudoprost broj u bazi** a.

Provjera prostosti neparnog broja $n > 2$ Solovay – Strassenovim testom započinje nasumičnim odabirom baze $a \in \{2, \ldots, n-1\}$. Potom se provjerava je li umnožak Jacobijevog simbola $\left(\frac{a}{n}\right)$ i vrijednosti $a^{\frac{n-1}{2}}$ kongruentan 1 modulo n. Test provodimo k puta i ukoliko se u nekoj iteraciji dogodi da taj umnožak nije kongruentan 1 modulo n, zaključujemo da je n složen. U suprotnom, n je vjerojatno prost.

Algoritam Solovay – Strassenovog testa izgleda ovako ([12]):

Algoritam 7 Solovay – Strassenov algoritam

input: odd number $n > 3$, $k \in \mathbb{N}$
for $i = 1$ to k **do**
  choose random $a \in \{2, \ldots, n-1\}$
  if $\left(\frac{a}{n}\right) a^{\frac{n-1}{2}} \not\equiv 1 \pmod{n}$ **then**
    return composite
return probably prime

U jednoj iteraciji Solovay – Strassenovog testa vjerojatnost da će složen broj netočno biti proglašen vjerojatno prostim manja je od $\frac{1}{2}$, a greška se smanjuje povećanjem broja iteracija. Dakle, za k nezavisnih iteracija greška je manja od $\left(\frac{1}{2}\right)^k$.

Usporedimo sve prethodno spomenute testove s obzirom na karakteristike u uvodnom dijelu poglavlja:

	opći	**deterministčan**	**bezuvjetan**	**polinomijalan**
Probno dijeljenje	+	+	+	−
AKS test	+	+	+	+
Lucas – Lahmerov test	−	+	+	+
Pepinov test	−	+	+	+
Fermatov test	+	−	+	+
Miller – Rabinov test	+	−	+	+
Solovay – Strassenov test	+	−	+	+

Tablica 3.1: Usporedba testova prostosti

3.3 Dokazivanje prostosti pomoću eliptičkih krivulja

Ideju dokazivanja prostosti pomoću eliptičkih krivulja 1986. godine predstavili su računalna znanstvenica **Shafi Goldwasser** i znanstvenik **Joe Kilian**, a iste godine ju je matematičar **Arthur Atkin** (1925. – 2008.) pretvorio u algoritam. Teorija vezana uz eliptičke krivulje opširna je i složena pa ćemo u ovome poglavlju spomenuti samo najosnovnije pojmove vezane uz istu.

Prvo ćemo definirati pojmove potrebne za definiranje eliptičkih krivulja.

Definicija 23. *Neka je K neprazan skup na kojemu su definirane binarne operacije zbrajanja $+ : K \times K \to K$ i množenja $\cdot : K \times K \to K$. Uređena trojka $(K, +, \cdot)$ naziva se polje ako vrijede sljedeća svojstva:*

1. *$(K, +)$ je abelova grupa s neutralnim elementom e;*
2. *$(K \setminus \{e\}, \cdot)$ je abelova grupa;*
3. *množenje je distributivno u odnosu na zbrajanje.*

Definicija 24. *Neka je K polje u kojemu je 0 neutralni element za zbrajanje i 1 neutralni element za množenje. Karakteristika polja K, $char(K)$, najmanji je prirodan broj n za koji je $1 + 1 + \cdots + 1 = n \cdot 1 = 0$. Ako takav broj n ne postoji, kažemo da je K polje karakteristike 0.*

Definicija 25. *Neka je K polje karakteristike različite od 2 i 3 i neka je $f(x) = x^3 + ax + b$, $a, b \in K$, kubni polinom bez višestrukih korijena. Eliptička krivulja E nad poljem K, u oznaci $E(K)$, skup je svih točaka $(x, y) \in K \times K$ koje zadovoljavaju jednadžbu $y^2 = x^3 + ax + b$, zajedno s još jednim elementom kojega označavamo s $\mathcal{O}$ i nazivamo točka u beskonačnosti, tj.*

$$E(K) = \{(x, y) \in K \times K : y^2 = x^3 + ax + b,\ 4a^3 + 27b^2 \neq 0\} \cup \{\mathcal{O}\}.$$

Definicija zahtjeva da polje ne bude karakteristike 2 i 3 jer nad takvim poljima eliptička krivulja ima drukčiji oblik.
Nad poljem karakteristike 2 eliptička krivulja ima jedan od dva oblika:

$$y^2 + cy = x^3 + ax + b \quad \text{ili} \quad y^2 + xy = x^3 + ax^2 + b.$$

dok je nad poljem karakteristike 3 oblika:

$$y^2 = x^3 + ax^2 + bx + c.$$

Opći oblik jednadžbe eliptičke krivulje dan je izrazom:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

i naziva se Weierstrassova forma od E. Ona se supstitucijom varijabli (nadopunom na potpun kvadrat ili kub) transformira do jednadžbi koje smo gore naveli i čiji oblik nazivamo kratka Weierstrassova forma.

Zahtjev da kubni polinom nema višestrukih nultočaka ekvivalentan je uvjetu $4a^3 + 27b^2 \neq 0$, pri čemu se broj $D = -4a^3 - 27b^2$ naziva diskriminanta polinoma $f(x)$. Kada je

- $D \neq 0$, f ima sve različite nultočke,
- $D = 0$, f ima višestruke nultočke, tj. geometrijski gledano, ima špic ili čvor.

Kod općega oblika jednadžbe eliptičke krivulje traži se da svaka točka krivulje bude nesingularna, tj. da za barem jednu od parcijalnih derivacija vrijedi da je $\frac{\partial f}{\partial x} \neq 0$ ili $\frac{\partial f}{\partial y} \neq 0$, tj. geometrijski gledano, da u svakoj točki krivulje postoji tangenta.
Jedno je od najvažnijih svojstava eliptičkih krivulja to što se može uvesti operacija zbrajanja uz koju skup točaka krivulje postaje abelova grupa. Upravo je zbog toga potrebno uvesti točku u beskonačnosti $\mathcal{O}$ jer ona će u toj grupi biti neutralni element.

Općenito, neka je dana eliptička krivulja E nad poljem $\mathbb{F}_p$ jednadžbom $E : y^2 = x^3 + ax + b$ i neka su $P = (x_1, y_1), Q = (x_2, y_2) \in E(\mathbb{F}_p)$ njene dvije točke. Tada je $P + Q = (x_3, y_3)$ i vrijede sljedeće formule za zbrajanje:

Udvostručavanje točke $(P = Q)$	**Zbrajanje točaka** $(P \neq Q)$
$\lambda = \frac{3x_1^2+a}{2y_1} \pmod p$	$\lambda = \frac{y_2-y_1}{x_2-x_1} \pmod p$
$x_3 = \lambda^2 - 2x_1 \pmod p$	$x_3 = \lambda^2 - x_1 - x_2 \pmod p$
$y_3 = \lambda(x_1 - x_3) - y_1 \pmod p$	$y_3 = \lambda(x_1 - x_3) - y_1 \pmod p$

Napomena 2. *Uočimo:*

- *kod udvostručavanja točke, prilikom računanja λ, mora vrijediti da je $y_1 \neq 0$. U slučaju da je $y_1 = 0$, vrijedit će da je $[2]P = P + P = \mathcal{O}$.*
- *kod zbrajanja točaka, prilikom računanja λ, mora vrijediti da je $x_2 - x_1 \neq 0$. U slučaju da je $x_2 - x_1 = 0$ i $y_2 \neq y_1$, vrijedit će da je $P + Q = \mathcal{O}$.*

Napokon, test prostosti pomoću eliptičkih krivulja dan je u sljedećem teoremu:

Teorem 20 (vidi [10]). *Neka je E eliptička krivulja nad $\mathbb{Z}_n$, gdje je $(6, n) = 1$ i $n > 1$, dana jednadžbom $y^2 = x^3 + ax + b$. Neka je $m \in \mathbb{N}$ koji ima prosti djelitelj $q > \left(n^{\frac{1}{4}} + 1\right)^2$. Ako postoji točka $P \in E(\mathbb{Z}_n)$ takva da je*

$$[m]P = \mathcal{O} \quad i \quad \left[\frac{m}{q}\right] P \neq \mathcal{O},$$

onda je n prost.

- Uvjet $(6, n) = 1$ osigurava da karakteristika od $\mathbb{Z}_n$ nije 2 ili 3.
- Ocjena za prosti djelitelj $q > \left(n^{\frac{1}{4}} + 1\right)^2$ proizlazi iz Hasseovog teorema[1] i osigurava da q bude dovoljno velik u odnosu na n.

[1] **Teorem** (Hasse). $q + 1 - 2\sqrt{q} \leq |E(\mathbb{F}_q)| \leq q + 1 + 2\sqrt{q}$.

- $[m]P = \underbrace{P + P + \cdots + P}_{m \text{ puta}}$ predstavlja točku dobivenu zbrajanjem točke P sa samom sobom m puta.
  $[m]P = \mathcal{O}$ znači da je točka P reda m na eliptičkoj krivulji.

Koraci za dokazivanje prostosti pomoću eliptičkih krivulja:

1. Odaberi broj n takav da je $n > 1$ i $(6, n) = 1$.
2. Odaberi prikladnu eliptičku krivulju E nad $\mathbb{Z}_n$ oblika $y^2 = x^3 + ax + b \pmod{n}$, gdje su $a, b \in \mathbb{Z}_n$. Provjeri uvjet $D = -4a^3 - 27b^2 \not\equiv 0 \pmod{n}$.
3. Odaberi točku $P = (x_1, y_1) \in E(\mathbb{Z}_n)$.
4. Izračunaj red m točke P, tj. odredi najmanji broj za koji je $[m]P = \mathcal{O}$.
5. Odredi prosti faktor q od m koji zadovoljava $q > \left(n^{\frac{1}{4}} + 1\right)^2$.
6. Provjeri jesu li zadovoljeni uvjeti Teorema 20:

$$[m]P = \mathcal{O} \quad \text{i} \quad \left[\frac{m}{q}\right] P \neq \mathcal{O}$$

Ova metoda prikladna je za primjenu na velikim brojevima n čiju prostost želimo dokazati. Za male brojeve nije efikasna zbog prirode prostoga faktora q. Detaljnije se o eliptičkim krivuljama može pročitati u ([10]) i ([9]).

4 | Primjena prostih brojeva

Najveću primjenu prostih brojeva pronalazimo u kriptografiji - znanstvenoj disciplini koja proučava metode slanja poruka zapisanih u obliku u kojemu ih samo osoba kojoj su namijenjene može pročitati.

Putem (nesigurnog) komunikacijskog kanala dvije osobe - **pošiljatelj** i **primatelj** razmjenjuju poruke. Poruka koju pošiljatelj želi poslati zove se **otvoreni tekst**. Kako bi svoju poruku učinio nerazumljivom trećoj osobi (**protivnik**) koja nadzire komunikacijski kanal, pošiljatelj će otvoreni tekst **šifrirati** (enkripcija) pomoću ranije dogovorenoga **ključa** i dobiti **šifrat** koji šalje primatelju. Ukoliko protivnik uspije doći do sadržaja šifrata, njemu on neće biti razumljiv, dok će primatelj koji zna kojim je ključem poruka šifrirana moći **dešifrirati** (dekripcija) primljeni šifrat i dobiti izvornu poruku, tj. otvoreni tekst.

Definicija 26. *Kriptosustav je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju vrijedi:*

1. $\mathcal{P}$ *je konačan skup svih mogućih osnovnih elemenata otvorenoga teksta;*
2. $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elemenata šifrata;*
3. $\mathcal{K}$ *je konačan skup svih mogućih ključeva;*
4. $\mathcal{E}$ *je skup svih funkcija šifriranja;*
5. $\mathcal{D}$ *je skup svih funkcija dešifriranja;*
6. *Za svaki ključ* $K \in \mathcal{K}$ *postoji funkcija šifriranja* $e_K \in \mathcal{E}$ *i odgovarajuća funkcija dešifriranja* $d_K \in \mathcal{D}$. *Pri tome su* $e_K : \mathcal{P} \to \mathcal{C}$ *i* $d_K : \mathcal{C} \to \mathcal{P}$ *funkcije sa svojstvom da je* $d_K(e_K(x)) = x$ *za svaki otvoreni tekst* $x \in \mathcal{P}$.

Napomena 3. *Iz posljednjeg svojstva Definicije 26 slijedi da funkcije* e_K *i* d_K *moraju biti injekcije. Kada bi se dogodilo da je*

$$e_K(x_1) = e_K(x_2) = y$$

za dva različita otvorena teksta x_1 *i* x_2, *onda primatelj poruke ne bi znao je li* $d_K(y) = x_1$ *ili* $d_K(y) = x_2$.

Kriptosustavi mogu se klasificirati prema nekoliko kriterija, a za ovaj rad najzanimljivija je klasifikacija s obzirom na tajnost ključeva. Prema tome, oni mogu biti:

- **simetrični** (kriptosustavi s tajnim ključem) kod kojih se ključ za dešifriranje može izračunati pomoću ključa za šifriranje i obrnuto. Najčešće su ti ključevi identični pa sigurnost ovakih kriptosustava leži u tajnosti ključa.
- **asimetrični** (kriptosustavi s javnim ključem) kod kojih se ključ za dešifriranje ne može u nekom razumnom vremenu izračunati iz ključa za šifriranje. Kod ovakvih kriptosustava ključ za šifriranje je javan, a ključ za dešifriranje tajan.

Jedan od najpoznatijih asimetričnih kriptosustava naziva se **RSA kriptosustav**. Njega su 1977. godine razvili **Ronald Rivest**, **Adi Shamir** i **Leonard Adleman**, a ideja iza njega je sljedeća:

Pretpostavimo da **Alice** i **Bob** žele razmjenjivati poruke. Neka Alice ima par generiranih ključeva (e_A, d_A), dok Bobu pripada par ključeva (e_B, d_B), pri čemu je prvi element u ključu javni, a drugi tajni. Prije nego što krenu slati poruke jedno drugome, međusobno će razmijeniti javne ključeve. Sada Alice ima par ključeva (e_B, d_A), a Bob (e_A, d_B). Ako Alice želi poslati poruku x Bobu, najprije će pomoću njegovoga javnog ključa e_B šifrirati svoju poruku:

$$e_B(x) = y.$$

Kada Bob dobije poruku y, dešifrirat će ju vlastitim tajnim ključem d_B i tako dobiti izvornu poruku x:

$$d_B(y) = d_B(e_B(x)) = x.$$

U slučaju da on želi odgovoriti na poruku, prvo će ju šifrirati njezinim javnim ključem e_A kako bi ju ona svojim tajnim ključem d_A mogla dešifrirati.

Definicija RSA kriptosustava je sljedeća:

Definicija 27. *Neka je $n = pq$, gdje su p i q prosti brojevi. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ i*

$$\mathcal{K} = \{(n, p, d, q, e) : n = pq,\ p, q \text{ prosti},\ de \equiv 1 \pmod{\varphi(n)}\}.$$

Za $K = (n, p, q, d, e) \in \mathcal{K}$ definiramo

$$e_K(x) = x^e \pmod{n}$$
$$d_K(y) = y^d \pmod{n},$$

pri čemu su $x, y \in \mathbb{Z}_n$.

U prethodnoj je definiciji φ Eulerova funkcija te je $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$. Javni ključ je (n, e), a (p, q, d) je tajni.
Sigurnost RSA kriptosustava oslanja se na težinu faktorizacije broja $n = pq$ pa je nužno da on bude dovoljno velik. Protivnik kojemu je poznat javni ključ (n, e) ni na koji način, u razumnom vremenskom okviru i uporabom trenutno dostupne tehnologije, ne može doći do tajnoga ključa (p, q, d).

RSA kriptosustavi koriste 1024 ili 2048-bitne veličine ključeva i do sada još nisu bili razbijeni. Vjeruje se kako bi se to u bliskoj budućnosti moglo dogoditi za 1024-bitne ključeve te se zbog veće razine sigurnosti predlaže duljina ključa od barem 2048 bita.
U posljednje vrijeme sve veću popularnost među kriptosustavima dobiva kriptosustav temeljen na eliptičkim krivuljama (*engl. Elliptic Curve Cryptosystem* - **ECC**). ECC pruža jednaku razinu sigurnosti, ali koristi manje memorije. Na primjer ključ veličine 4096 bita u RSA sustavu daje jednaku razinu sigurnosti kao 313 bitni ključ u ECC-u. Više o tome može se pronaći u ([4]) i ([21]).

5 | Slutnje o prostim brojevima

Teorija brojeva grana je matematike s najpoznatijim i najdugovječnijim nedokazanim slutnjama. Među njima je i ranije spomenuta Riemannova slutnja (Slutnja 1) koja umove matematičara zaokuplja već 165 godina. Osim nje, u prethodnim smo poglavljima spomenuli njih nekoliko, a u ovome ćemo navesti još neke poznate slutnje vezane uz proste brojeve.

Definicija 28. *Za par brojeva $(p, p+2)$ kažemo da su prosti brojevi blizanci ukoliko su oba p i $p+2$ prosti brojevi.*

Slutnja 3 (de Polignacova slutnja, vidi [17])**.** *Postoji beskonačno mnogo prostih brojeva p takvih da je i $p+2$ također prost broj.*

Primjer 10. *Prvih nekoliko parova prostih brojeva blizanaca:*

$$(3,5),(5,7),(11,13),(17,19),(29,31),\ldots.$$

U rujnu 2016. godine pronađen je novi par prostih brojeva blizanaca:

$$(2\,996\,863\,034\,895 \cdot 2^{1\,290\,000} - 1, 2\,996\,863\,034\,895 \cdot 2^{1\,290\,000} + 1),$$

a svaki ima 388 342 znamenke.

Slutnja 4 (Lagrangeova slutnja, vidi [17])**.** *Svaki se neparan prirodan broj > 5 može zapisati kao suma $p + 2q$, pri čemu su oba p i q prosti brojevi.*

Primjer 11. *Prvih nekoliko neparnih prirodnih brojeva > 5 koji zadovoljavaju Lagrangeovu slutnju:*

$$\begin{aligned} 7 &= 3 + 2 \cdot 2, \\ 9 &= 5 + 2 \cdot 2, \\ 11 &= 5 + 2 \cdot 3, \\ 13 &= 3 + 2 \cdot 5, \\ 15 &= 5 + 2 \cdot 5, \\ &\vdots \end{aligned}$$

Slutnja 5 (Goldbachova slutnja, vidi [17])**.** *Svaki se paran broj > 2 može zapisati kao suma dva prosta broja.*

Primjer 12. *Prvih nekoliko parnih brojeva* > 2 *koji zadovoljavaju Goldbachovu slutnju:*

$$\begin{aligned} 4 &= 2+2, \\ 6 &= 3+3, \\ 8 &= 3+5, \\ 10 &= 3+7 = 5+5, \\ 12 &= 5+7, \\ &\vdots \end{aligned}$$

Slutnja 6 (Landauova slutnja, vidi [17])**.** *Postoji beskonačno mnogo prostih brojeva oblika* n^2+1*.*

Primjer 13. *Prvih nekoliko prostih brojeva oblika* n^2+1*:*

$$\begin{aligned} n = 1 &\Rightarrow 1^2+1 = 2, \\ n = 2 &\Rightarrow 2^2+1 = 5, \\ n = 4 &\Rightarrow 4^2+1 = 17, \\ n = 6 &\Rightarrow 6^2+1 = 37, \\ n = 10 &\Rightarrow 10^2+1 = 101, \\ &\vdots \end{aligned}$$

Literatura

[1] W. R. Alford, A. Granville, C. Pomerance, *There are infinitely many Carmichael numbers*, Annals of Mathematics, **140**(1994), 103–722.

[2] M. Agrawal, N. Kajal, N. Saxena, *PRIMES is in P*, Annals of Mathematics, **160**(2004), 781–793.

[3] J. Barthel, P. Sgobba, F. Zhu, *Visualizing the distribution of primes*, dostupno na `\https://math.uni.lu/eml/assets/reports/prime-distribution.pdf`.

[4] I. F. Blake, G. Seroussi, N. P. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press, Cambridge, 1999.

[5] F. M. Brückler, *Povijest matematike II*, Sveučilište J. J. Strossmayera u Osijeku - Odjel za matematiku, Osijek, 2010.

[6] D. M. Burton, *Elementary Number Theory (7th ed.)*, McGraw-Hill Companies Inc., New York, 2011.

[7] K. Conrad, *Carmichael numbers and Korselt's criterion*, dostupno na `\https://kconrad.math.uconn.edu/blurbs/ugradnumthy/carmichaelkorselt.pdf`

[8] B. Conrey, *Riemann's hypothesis*, dostupno na `\https://aimath.org/~kaur/publications/90.pdf`.

[9] R. Crandall, C. Pomerance, *Prime Numbers: A Computational Perspective (2nd ed.)*, Springer, 2000.

[10] A. Dujella, *Eliptičke krivulje u kriptografiji*, skripta, PMF - MO, Sveučilište u Zagrebu, 2013., dostupno na `\https://web.math.pmf.unizg.hr/~duje/elkript/elkripto2.pdf`.

[11] P. Erdös, *On a new method in elementary number theory which leads to an elementary proof of the prime number theorem*, Proceedings of the National Academy of Science, **35.7**(1949), 374–384.

[12] J. Gallier, J. Quantance, *Notes on Primality Testing And Public Key Cryptography Part 1: Randomized Algorithms: Miller–Rabin and Solovay–Strassen Tests*, Department of Computer and Information Science, University of Pennsylvania, Philadelphia, 2024.

[13] T. Koshy, *Elementary Number Theory with Applications (2nd ed.)*, Academic Press, Burlington, 2007.

[14] I. Matić, *Uvod u teoriju brojeva*, Sveučilište J. J. Strossmayera u Osijeku - Odjel za matematiku, Osijek, 2015.

[15] G. Savin, *Numbers, Groups and Cryptography*, skripta, Department of Mathematics, University of Utah, 2009.

[16] A. Selberg, *An Elementary Proof of the Prime - Number Theorem*, Annals of Mathematics, Second Series, **50.2**(1949), 305–313.

[17] K. Singh, *Number Theory: Step by Step*, Oxford University Press, Oxford, 2020.

[18] N. Stamatopoulos, Z. Wu, *Chebyshev's theorem on the distribution of prime numbers*, ETH Zürich, 2021., dostupno na `\https://metaphor.ethz.ch/x/2021/hs/401-3110-71L/ex/eighth.pdf`.

[19] W. Stein, *Fermat Numbers*, University of Washington, Washington, 2010.

[20] J. J. Tattersall, *Elementary Number Theory in Nine Chapters (2nd ed.)*, Cambridge University Press, Cambridge, 2005.

[21] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography (2nd ed.)*, Chapman & Hall/CRC, New York, 2008.

[22] R. Worthington, *Primality Testing - Theory, Complexity and Applications*, Whitman College, Washington, 2018.

[23] S. Y. Yan, *Number Theory for Computing*, Springer, Berlin, 2002.

[24] D. Zagier, *Newman's Short Proof of the Prime Number Theorem*, Mathematical Association of America, The Mathematical Monthly, **104.8**(1997), 705–708.

Sažetak

Tema ovoga rada prosti su brojevi. Iako su u početku proučavani isključivo iz teorijske perspektive, pojava digitalnih računala donijela je potrebu za zaštitom podataka i sigurnošću u svakodnevnoj komunikaciji, gdje su prosti brojevi pronašli svoju praktičnu primjenu. U ovome radu prosti se brojevi gledaju iz oba kuta - teorijskoga i praktičnoga. Prvi dio pokriva definiciju prostih brojeva, njihova osnovna svojstva te proste brojeve posebnoga oblika, dok je drugi dio usmjeren na testove prostosti i primjenu prostih brojeva u kriptografiji. Cijeli rad zaokružen je poglavljem o još uvijek nedokazanim slutnjama u teoriji brojeva, a koji su vezane uz proste brojeve.

Ključne riječi

prosti brojevi, osnovni teorem aritmetike, Fermatovi prosti brojevi, Mersenneovi prosti brojevi, Sophieini prosti brojevi, teorem o prostim brojevima, testovi prostosti, RSA kriptosustav

Prime numbers

Summary

The topic of this paper is prime numbers. Although initially studied purely from a theoretical perspective, the advent of digital computers brought about a need for data protection and security in daily communications, where prime numbers found their practical application. This paper examines prime numbers from both theoretical and practical angles. The first part covers the definition, basic properties and special forms of prime numbers, while the second part focuses on primality tests and application of prime numbers in cryptography. The paper concludes with a discussion on unproven hypotheses in number theory related to prime numbers.

Keywords

prime numbers, fundamental theorem of arithmetic, Fermat's primes, Mersenne's primes, Germain primes, prime number theorem, primality testing, RSA cryptosystem

Životopis

Rođena sam 31. kolovoza 1996. godine u Osijeku. Osnovnu školu Franje Krežme u Osijeku pohađala sam u razdoblju od 2004. do 2011. godine, a nakon toga obrazovanje nastavljam u I. gimnaziji Osijek. Fakultet primijenjene matematike i informatike (tadašnji Odjel za matematiku) upisala sam 2015. godine.